सत्यमेव जयते

टीईसी 26053:2022

टीएसडीएसआई मानक T1.3GPP 23.288-17.4.0 V1.0.0से अभिग्रहण

TEC 26053:2022

Adopted from TSDSI STD T1.3GPP 23.288-17.4.0 V1.0.0

नेटवर्क डेटा एनालिटिक्स सेवाओं का समर्थन करने के लिए 5 जी सिस्टम (5 जीएस) के लिए आर्किटेक्चर एन्हांसमेंट

Architecture enhancements for 5G System (5GS) to support network data analytics services

ISO 9001:2015

दूरसंचारअभियांत्रिकीकेंद्र

खुर्शीद लालभवन, जनपथ, नईदिल्ली-110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHID LAL BHAWAN, JANPATH, NEW DELHI-110001, IND

www.tec.gov.in

About TEC

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centres (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

©टीईसी, 2022

©TEC, 2022

इस सर्वाधिकार सुरक्षित प्रकाशन का कोई भी हिस्सा, दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली की लिखित स्वीकृति के बिना, किसी भी रूप में या किसी भी प्रकार से जैसे -इलेक्ट्रॉनिक, मैकेनिकल,फोटोकॉपी, रिकॉर्डिंग, स्कैनिंग आदि रूप में प्रेषित, संग्रहीत या पुनरुत्पादित न किया जाए ।

All rights reserved and no part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form and by any means - electronic, mechanical, photocopying, recording, scanning or otherwise, without written permission from the Telecommunication Engineering Centre, New Delhi.

Release: June,2022

ABSTRACT

The present document defines the Stage 2 architecture enhancements for 5G System (5GS) to support network data analytics services in 5G Core network.

HISTORY SHEET

Sl. No.	Document Number	Title	Remarks
1.	TEC 26053:2022 TSDSI STD T1.3GPP 23.288-17.4.0 V1.0.0	Architecture enhancements for 5G System (5GS) to support network data analytics services	

,

Contents

Foreword....8

1 Scope....9

2 References....9

3 Definitions and abbreviations....10
3.1 Definitions....10
3.2 Abbreviations....10

4 Reference Architecture for Data Analytics....10
4.1 General....10
4.2 Non-roaming architecture....11
4.2.0 General....11
4.2.1 Analytics Data Repository Function....13
4.3 Roaming architecture....14

5 Network Data Analytics Functional Description....14
5.1 General....14
5.2 NWDAF Discovery and Selection....15

5A Data Collection Coordination and Delivery Functional Description....17
5A.1 General....17
5A.2 Data Collection Coordination....17
5A.3 Data Delivery....18
5A.3.1 Data Delivery via the DCCF....19
5A.3.2 Data Delivery via a Messaging Framework....20
5A.4 Data Formatting and Processing....21
5A.5 Historical Data Handling....22

5B Analytics Data Repository Functional Description....23
5B.1 General....23

6 Procedures to Support Network Data Analytics....24
6.0 General....24
6.1 Procedures for analytics exposure....24
6.1.1 Analytics Subscribe/Unsubscribe....24
6.1.1.1 Analytics subscribe/unsubscribe by NWDAF service consumer....24
6.1.1.2 Analytics subscribe/unsubscribe by AFs via NEF....24
6.1.2 Analytics Request....26
6.1.2.1 Analytics request by NWDAF service consumer....26
6.1.2.2 Analytics request by AFs via NEF....26
6.1.3 Contents of Analytics Exposure....27
6.1.4 Analytics Exposure using DCCF....30
6.1.4.1 General....30
6.1.4.2 Analytics Exposure via DCCF....30
6.1.4.3 Historical Analytics Exposure via DCCF....32
6.1.4.4 Analytics Exposure via Messaging Framework....34
6.1.4.5 Historical Analytics Exposure via Messaging Framework....36
6.1A Analytics aggregation from multiple NWDAFs....38
6.1A.1 General....38
6.1A.2 Analytics Aggregation....39
6.1A.3 Procedure for analytics aggregation....39
6.1A.3.1 Procedure for analytics aggregation with Provision of Area of Interest....39
6.1A.3.2 Procedure for Analytics Aggregation without Provision of Area of Interest....41
6.1B Transfer of analytics context and analytics subscription....43
6.1B.1 General....43
6.1B.2 Analytics Transfer Procedures....44
6.1B.2.1 Analytics context transfer initiated by target NWDAF selected by the NWDAF service consumer....44
6.1B.2.2 Analytics Subscription Transfer initiated by source NWDAF....45

6.1B.2.3 Prepared analytics subscription transfer ... 48
6.1B.3 Analytics Context Transfer ... 50
6.1B.4 Contents of Analytics Context ... 51
6.1C NWDAF Registration/Deregistration in UDM ... 52
6.1C.1 General ... 52
6.1C.2 NWDAF Registration in UDM ... 52
6.1C.3 NWDAF De-registration from UDM ... 53
6.2 Procedures for Data Collection ... 53
6.2.1 General ... 53
6.2.2 Data Collection from NFs ... 55
6.2.2.1 General ... 55
6.2.2.2 Procedure for Data Collection from NFs ... 59
6.2.2.3 Procedure for Data Collection from AF via NEF ... 60
6.2.2.4 Procedure for Data Collection from NRF ... 62
6.2.2.5 Usage of Exposure framework by the NWDAF for Data Collection ... 62
6.2.3 Data Collection from OAM ... 63
6.2.3.1 General ... 63
6.2.3.2 Procedure for data collection from OAM ... 63
6.2.4 Correlation between network data and service data ... 64
6.2.5 Time coordination across multiple NWDAF instances ... 65
6.2.5.1 General ... 65
6.2.5.2 Procedure for time coordination across multiple NWDAFs ... 66
6.2.6 Enhanced Procedures for Data Collection ... 67
6.2.6.0 General ... 67
6.2.6.1 Bulked Data Collection ... 67
6.2.6.1.0 General ... 67
6.2.6.1.1 Services for Bulked Data Collection ... 68
6.2.6.2 Procedure for Data Collection from NWDAF ... 70
6.2.6.3 Data Collection using DCCF ... 73
6.2.6.3.1 General ... 73
6.2.6.3.2 Data Collection via DCCF ... 73
6.2.6.3.3 Historical Data Collection via DCCF ... 76
6.2.6.3.4 Data Collection via Messaging Framework ... 78
6.2.6.3.5 Historical Data Collection via Messaging Framework ... 80
6.2.6.3.6 Data collection profile registration ... 83
6.2.7 Data Collection with Event Muting Mechanism ... 84
6.2.7.1 General ... 84
6.2.7.2 Procedure for Data Collection with Event Muting Mechanism ... 84
6.2.8 Data Collection from the UE Application ... 86
6.2.8.1 General ... 86
6.2.8.2 Procedure for data collection from the UE Application ... 87
6.2.8.2.1 Connection establishment between UE Application and AF ... 87
6.2.8.2.2 AF registration and discovery ... 88
6.2.8.2.3 Data Collection Procedure from UE ... 88
6.2.8.2.4 Correlation between UE data collection and the NWDAF data request ... 89
6.2.8.2.4a Void ... 92
6.2.9 User consent for analytics ... 92
6.2A Procedure for ML Model Provisioning ... 93
6.2A.0 General ... 93
6.2A.1 ML Model Subscribe/Unsubscribe ... 93
6.2A.2 Contents of ML Model Provisioning ... 94
6.2A.3 ML Model request ... 95
6.2B Analytics Data Repository procedures ... 96
6.2B.1 General ... 96
6.2B.2 Historical Data and Analytics storage ... 96
6.2B.3 Historical Data and Analytics Storage via Notifications ... 97
6.2B.4 Data removal from an ADRF ... 98
6.3 Slice load level related network data analytics ... 98
6.3.1 General ... 98
6.3.2 Void ... 99
6.3.2A Input data ... 99
6.3.3 Void ... 100

6.3.3A Output analytics 100
6.3.4 Procedures 103
6.4 Observed Service Experience related network data analytics 104
6.4.1 General 104
6.4.2 Input Data 106
6.4.3 Output Analytics 108
6.4.4 Procedures to request Service Experience for an Application 111
6.4.5 Procedures to request Service Experience for a Network Slice 113
6.4.6 Procedures to request Service Experience for a UE 113
6.5 NF load analytics 114
6.5.1 General 114
6.5.2 Input data 115
6.5.3 Output analytics 117
6.5.4 Procedures 118
6.6 Network Performance Analytics 120
6.6.1 General 120
6.6.2 Input Data 121
6.6.3 Output Analytics 121
6.6.4 Procedures 123
6.7 UE related analytics 124
6.7.1 General 124
6.7.2 UE mobility analytics 124
6.7.2.1 General 124
6.7.2.2 Input Data 125
6.7.2.3 Output Analytics 126
6.7.2.4 Procedures 126
6.7.3 UE Communication Analytics 128
6.7.3.1 General 128
6.7.3.2 Input Data 129
6.7.3.3 Output Analytics 130
6.7.3.4 Procedures 131
6.7.4 Expected UE behavioural parameters related network data analytics 133
6.7.4.1 General 133
6.7.4.2 Input Data 134
6.7.4.3 Output Analytics 134
6.7.4.4 Procedures 134
6.7.4.4.1 NWDAF-assisted expected UE behavioural analytics 134
6.7.5 Abnormal behaviour related network data analytics 135
6.7.5.1 General 135
6.7.5.2 Input Data 136
6.7.5.3 Output Analytics 137
6.7.5.4 Procedure 139
6.8 User Data Congestion Analytics 140
6.8.1 General 140
6.8.2 Input data 141
6.8.3 Output analytics 142
6.8.4 Procedures 144
6.8.4.1 Procedure for one-time or continuous reporting of analytics for user data congestion in a geographic area 144
6.8.4.2 Procedure for one-time or continuous reporting of analytics for user data congestion for a specific UE 146
6.9 QoS Sustainability Analytics 149
6.9.1 General 149
6.9.2 Input data 150
6.9.3 Output analytics 150
6.9.4 Procedures 151
6.10 Dispersion Analytics 151
6.10.1 General 151
6.10.2 Input Data 153
6.10.3 Output Analytics 157
6.10.3.0 General 157
6.10.3.1 Data Volume Dispersion Analytics 157

6.10.3.2 Transactions Dispersion Analytics ... 161
6.10.4 Dispersion Analytic Procedure ... 164
6.11 WLAN performance analytics ... 166
6.11.1 General ... 166
6.11.2 Input Data ... 167
6.11.3 Output Analytics ... 168
6.11.4 Procedures ... 169
6.12 Session Management Congestion Control Experience Analytics ... 170
6.12.1 General ... 170
6.12.2 Input Data ... 170
6.12.3 Output Analytics ... 171
6.12.4 Procedures ... 171
6.13 Redundant Transmission Experience related analytics ... 172
6.13.1 General ... 172
6.13.2 Input Data ... 173
6.13.3 Output Analytics ... 173
6.13.4 Procedures ... 174
6.13.4.1 Analytics Procedure ... 174
6.14 DN Performance Analytics ... 176
6.14.1 General ... 176
6.14.2 Input Data ... 177
6.14.3 Output Analytics ... 178
6.14.4 Procedures to request DN Performance Analytics for an Application ... 179
6.15 Void ... 180

7 Nnwdaf Services Description ... 180
7.1 General ... 180
7.2 Nnwdaf_AnalyticsSubscription Service ... 183
7.2.1 General ... 183
7.2.2 Nnwdaf_AnalyticsSubscription_Subscribe service operation ... 183
7.2.3 Nnwdaf_AnalyticsSubscription_Unsubscribe service operation ... 184
7.2.4 Nnwdaf_AnalyticsSubscription_Notify service operation ... 184
7.2.5 Nnwdaf_AnalyticsSubscription_Transfer service operation ... 185
7.3 Nnwdaf_AnalyticsInfo service ... 186
7.3.1 General ... 186
7.3.2 Nnwdaf_AnalyticsInfo_Request service operation ... 186
7.3.3 Nnwdaf_AnalyticsInfo_ContextTransfer service operation ... 186
7.4 Nnwdaf_DataManagement Service ... 187
7.4.1 General ... 187
7.4.2 Nnwdaf_DataManagement_Subscribe service operation ... 187
7.4.3 Nnwdaf_DataManagement_Unsubscribe service operation ... 188
7.4.4 Nnwdaf_DataManagement_Notify service operation ... 188
7.4.5 Nnwdaf_DataManagement_Fetch service operation ... 188
7.5 Nnwdaf_MLModelProvision services ... 189
7.5.1 General ... 189
7.5.2 Nnwdaf_MLModelProvision_Subscribe service operation ... 189
7.5.3 Nnwdaf_MLModelProvision_Unsubscribe service operation ... 189
7.5.4 Nnwdaf_MLModelProvision_Notify service operation ... 189
7.6 Nnwdaf_MLModelInfo service ... 190
7.6.1 General ... 190
7.6.2 Nnwdaf_MLModelInfo_Request service operation ... 190

8 DCCF Services ... 190
8.1 General ... 190
8.2 Ndccf_DataManagement service ... 190
8.2.2 Ndccf_DataManagement_Subscribe service operation ... 191
8.2.3 Ndccf_DataManagement_Unsubscribe service operation ... 191
8.2.4 Ndccf_DataManagement_Notify service operation ... 191
8.2.5 Ndccf_DataManagement_Fetch service operation ... 192
8.3 Ndccf_ContextManagement service ... 192
8.3.1 General ... 192
8.3.2 Ndccf_ContextManagement_Register service operation ... 192

8.3.3 Ndccf_ContextManagement_Update service operation 193
8.3.4 Ndccf_ContextManagement_Deregister service operation 193

9 MFAF Services 193
9.1 General 193
9.2 Nmfaf_3daDataManagement service 193
9.2.1 General 193
9.2.2 Nmfaf_3daDataManagement_Configure service operation 194
9.2.3 Nmfaf_3daDataManagement_Deconfigure service operation 194
9.3 Nmfaf_3caDataManagement service 194
9.3.1 General 194
9.3.2 Nmfaf_3caDataManagement_Notify service operation 194
9.3.3 Nmfaf_3caDataManagement_Fetch service operation 195

10 ADRF Services 195
10.1 General 195
10.2 Nadrf_DataManagement service 196
10.2.1 General 196
10.2.2 Nadrf_DataManagement_StorageRequest service operation 196
10.2.3 Nadrf_DataManagement_StorageSubscriptionRequest service operation 196
10.2.4 Nadrf_DataManagement_StorageSubscriptionRemoval service operation 196
10.2.5 Nadrf_DataManagement_RetrievalRequest service operation 197
10.2.6 Nadrf_DataManagement_RetrievalSubscribe service operation 197
10.2.7 Nadrf_DataManagement_RetrievalUnsubscribe service operation 198
10.2.8 Nadrf_DataManagement_RetrievalNotify service operation 198
10.2.9 Nadrf_DataManagement_Delete 198

Annex A (informative): Change history 199

Foreword

In pursuance of the Standardization Guide notified by TEC vide Office Memorandum No.2-1/2018/SD/TSDSI/TEC/5 dated 8th May 2020,this Technical Standard has been adopted as “identical adoption” based on request from TSDSI.The source documents is Technical Standard No.TSDSI STD T1.3GPP 36.101-10.25.0 V1.0.0, which is a transposed technical standard produced by TSDSI and the same was originally sourced by TSDSI from the technical specification produced by 3rd Generation Partnership Project (3GPP),of which TSDSI is an organizational Partner .This Technical Standard has been adopted as National Standard shall be voluntary unless made mandatory by its use, reference or adoption by regulation/government directive.

This Technical Standard has been transposed from the technical specification produced by the 3rd Generation Partnership Project (3GPP), of which, TSDSI is an Organizational Partner.

The contents of the 3GPP Specification document are subject to continuing work within the 3GPP TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the Stage 2 architecture enhancements for 5G System (5GS) to support network data analytics services in 5G Core network.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501:"System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[5] Void.

[6] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[7] 3GPP TS 28.550: "Management and orchestration; Performance Assurance".

[8] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[9] 3GPP TS 28.545: "Management and orchestration; Fault Supervision (FS)".

[10] 3GPP TS 28.554: "Management and orchestration; 5G end to end Key Performance Indicators (KPI)".

[11] ITU-T Recommendation P.1203.3: "Parametric bitstream-based quality assessment of progressive download and adaptive audiovisual streaming services over reliable transport - Quality integration module".

[12] 3GPP TS 38.215: "NR; Physical layer measurements".

[13] Void.

[14] 3GPP TS 38.331: "NR; Radio Resource Control (RRC) protocol specification".

[15] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[16] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[17] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes".

[18] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[19] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[20] 3GPP TS 37.320: "Radio measurement collection for Minimization of Drive Tests (MDT); Overall description; stage 2".

[21] 3GPP TS 28.201: "Charging management; Network slice performance and analytics charging in the 5G System (5GS); stage 2".

[22] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[23] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[24] 3GPP TS 28.310: "Management and orchestration; Energy efficiency of 5G".

[25] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[26] 3GPP TS 29.503: "Unified Data Management Services; Stage 3".

[27] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[28] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[29] 3GPP TS 26.118: "Virtual Reality (VR) profiles for streaming applications".

[30] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[31] 3GPP TS 26.512: "5G Media Streaming (5GMS); Protocols".

[32] 3GPP TS 26.531: "Data Collection and Reporting; General Description and Architecture".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1], TS 23.501 [2] and TS 23.503 [4]. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 23.501 [2] and TS 23.503 [4] apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

4 Reference Architecture for Data Analytics

4.1 General

The NWDAF (Network Data Analytics Function) is part of the architecture specified in TS 23.501 [2] and uses the mechanisms and interfaces specified for 5GC in TS 23.501 [2] and OAM services (see clause 6.2.3.1).

The NWDAF interacts with different entities for different purposes:

- Data collection based on subscription to events provided by AMF, SMF, PCF, UDM, AF (directly or via NEF), and OAM;
- [Optionally] Analytics and Data collection using the DCCF (Data Collection Coordination Function);
- Retrieval of information from data repositories (e.g. UDR via UDM for subscriber-related information);

- [Optionally] Storage and retrieval of information from ADRF (Analytics Data Repository Function);
- [Optionally] Analytics and Data collection from MFAF (Messaging Framework Adaptor Function);
- Retrieval of information aboutNFs (e.g. from NRF for NF-related information);
- On demand provision of analytics to consumers, as specified in clause 6.
- Provision of bulked data to consumers, as specified in clause 6.

A single instance or multiple instances of NWDAF may be deployed in a PLMN. If multiple NWDAF instances are deployed, the architecture supports deploying the NWDAF as a central NF, as a collection of distributed NFs, or as a combination of both. If multiple NWDAF instances are deployed, an NWDAF can act as an aggregate point (i.e. Aggregator NWDAF) and collect analytics information from other NWDAFs, which may have different Serving Areas, to produce the aggregated analytics (per Analytics ID), possibly with Analytics generated by itself.

NOTE 1: When multiple NWDAFs exist, not all of them need to be able to provide the same type of analytics results, i.e. some of them can be specialized in providing certain types of analytics. An Analytics ID information element is used to identify the type of supported analytics that NWDAF can generate.

NOTE 2: NWDAF instance(s) can be collocated with a 5GS NF.

4.2 Non-roaming architecture

4.2.0 General

As depicted in Figure 4.2.0-1, the 5G System architecture allows NWDAF to collect data from any 5GC NF. The NWDAF belongs to the same PLMN as the 5GC NF that provides the data.

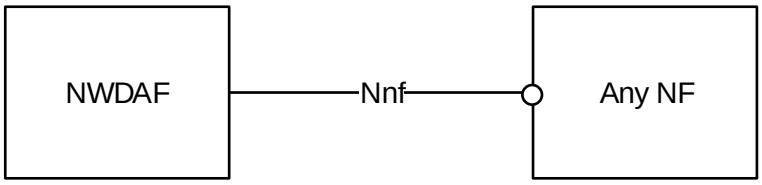

Figure 4.2.0-1: Data Collection architecture from any 5GC NF

The Nnf interface is defined for the NWDAF to request subscription to data delivery for a particular context, to cancel subscription to data delivery and to request a specific report of data for a particular context.

The 5G System architecture allows NWDAF to retrieve the management data from OAM by invoking OAM services.

The 5G System architecture allows NWDAF to collect data from any 5GC NF or OAM using a DCCF with associated Ndccf services as specified in clause 8.2.

The 5G System architecture allows NWDAF and DCCF to collect data from an NWDAF with associated Nnwdaf_DataManagement services as specified in clause 7.4. The 5G system architecture allows MFAF to fetch data from an NWDAF with associated Nnwdaf_DataManagement service as specified in clause 7.4.

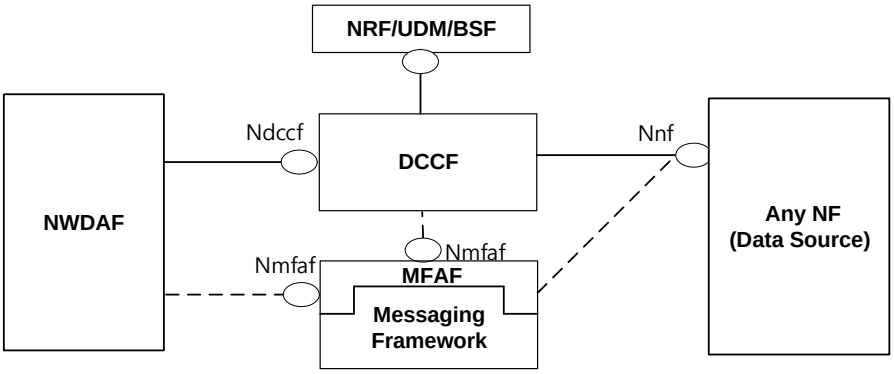

Figure 4.2.0-1a: Data Collection architecture using Data Collection Coordination

As depicted in Figure 4.2.0-1a, the Ndccf interface is defined for the NWDAF to support subscription request(s) for data delivery from a DCCF, to cancel subscription to data delivery, and to request a specific report of data. If the data is not already being collected, the DCCF requests the data from the Data Source using Nnf services. The DCCF may collect the data and deliver it to the NWDAF or the DCCF may rely on a messaging framework to collect data from the NF and deliver it to the NWDAF.

As depicted in Figure 4.2.0-2, the 5G System architecture allows any 5GC NF to request network analytics information from NWDAFcontaining Analytics logical function (AnLF). The NWDAF belongs to the same PLMN as the 5GC NF that consumes the analytics information.

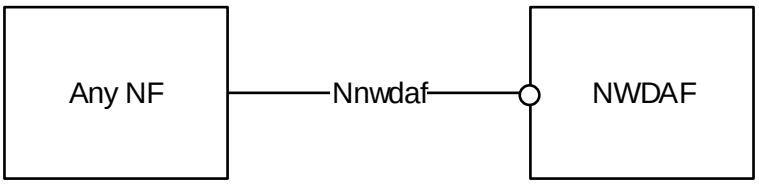

Figure 4.2.0-2: Network Data Analytics Exposure architecture

The Nnwdaf interface is defined for 5GC NFs, to request subscription to network analytics delivery for a particular context, to cancel subscription to network analytics delivery and to request a specific report of network analytics for a particular context.

NOTE 1: The 5G System architecture also allows other consumers such as OAM and CEF (Charging Enablement Function) to request network analytics information from NWDAF.

The 5G System architecture allows any NF to obtain Analytics from an NWDAF using a DCCF function with associated Ndccf services, as specified in clause 8.2.

The 5G System architecture allows NWDAF and DCCF to request historical analytics from an NWDAF with associated Nnwdaf_DataManagement services as specified in clause 7.4. The 5G system architecture allows MFAF to fetch historical analytics from an NWDAF with associated Nnwdaf_DataManagement service as specified in clause 7.4.

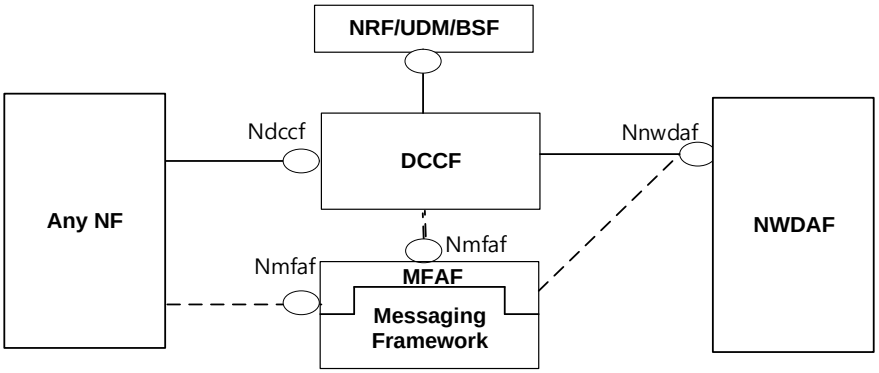

Figure 4.2.0-2a: Network Data Analytics Exposure architecture using Data Collection Coordination

As depicted in Figure 4.2.0-2a, the Ndccf interface is defined for any NF to support subscription request(s) to network analytics, to cancel subscription for network analytics, and to request a specific report of network analytics. If the analytics is not already being collected, the DCCF requests the analytics from the NWDAF using Nnwdaf services. The DCCF may collect the analytics and deliver it to the NF, or the DCCF may rely on a messaging framework to collect analytics and deliver it to the NF.

As depicted in Figure 4.2.0-3, the 5G System architecture allows NWDAF containing Analytics logical function (AnLF) to use trained ML model provisioning services from another NWDAF containing Model Training logical function (MTLF).

NOTE 2: Analytics logical function and Model Training logical function are described in clause 5.1.

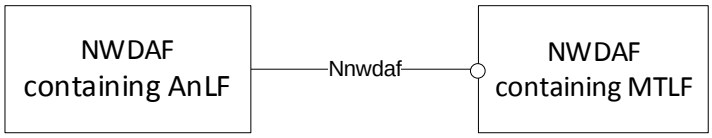

Figure 4.2.0-3: Trained ML Model Provisioning architecture

The Nnwdaf interface is used by an NWDAF containingAnLF to request and subscribe to trained ML model provisioning services.

NOTE 3: The NWDAF trained ML model provisioning services are described in clause 7.5 and clause 7.6.

NOTE 4: The NWDAF containing AnLF is the only consumer of trained ML model provisioning services in this release of the specification.

4.2.1 Analytics Data Repository Function

As depicted in Figure 4.2.1-1, the 5G System architecture allows ADRF to store and retrieve the collected data and analytics. The following options are supported:

- ADRF exposes the Nadrf service for storage and retrieval of data by other 5GC NFs (e.g. NWDAF) which access the data using Nadrf services.
- Based on the NF request or configuration on the DCCF, the DCCF may determine the ADRF and interact directly or indirectly with the ADRF to request or store data. The interaction can be:

- Direct: the DCCF requests to store data in the ADRF via an Nadrf service, or via an Ndccf_DataManagement_Notify (e.g. when ADRF requested data collection notification via DCCF). In addition, the DCCF retrieves data from the ADRF via an Nadrf service.

- Indirect: the DCCF requests that the Messaging Framework to store data in the ADRF i.e. via an Nadrf service or via an Nmfaf_3daDataManagement_Configure. The Messaging Framework may contain one or more Adaptors that translate between 3GPP defined protocols.

NOTE 1: The internal logic of Messaging Framework is outside the scope of 3GPP, only the MFAF and the interface between MFAF and other 3GPP defined NF is under 3GPP scope.

- A Consumer NF may specify in requests to a DCCF that data provided by a Data Source needs to be stored in the ADRF.

- The ADRF stores data received in an Nadrf_DataManagement_StorageRequest sent directly from an NF, or data received in an Ndccf_DataManagement_Notify / Nmfaf_3caDataManagement_Notify or Nnwdaf_DataManagement_Notify from the DCCF, MFAF or from the NWDAF.

- The ADRF checks if the Data Consumer is authorized to access ADRF services and provides the requested data using the procedures specified in TS 23.501 [2] clause 7.1.4.

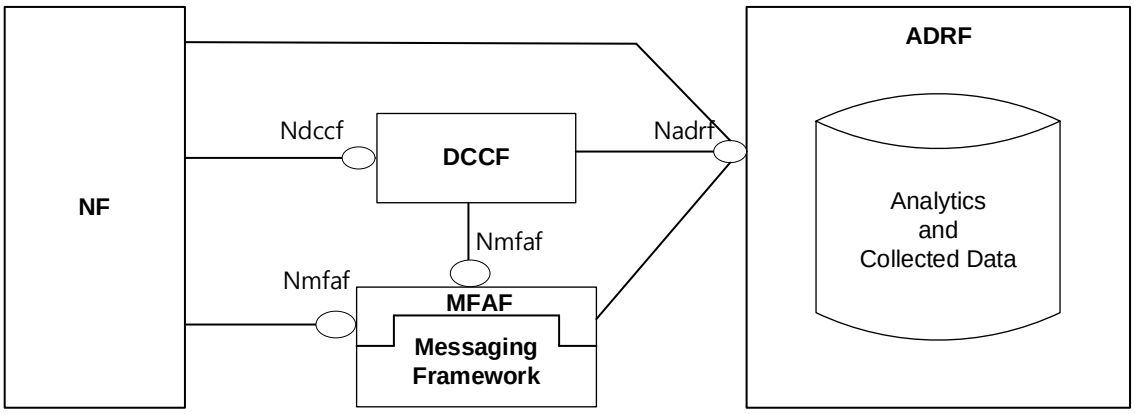

Figure 4.2.1-1: Data storage architecture for Analytics and Collected Data

4.3 Roaming architecture

The interactions between the NWDAF and the other 5GC NFs are only considered in the same PLMN case.

Roaming architecture does not apply in this release of the specification.

5 Network Data Analytics Functional Description

5.1 General

The NWDAF provides analytics to 5GC NFs, and OAM as defined in clause 7. An NWDAF may contain the following logical functions:

- **Analytics logical function (AnLF):** A logical function in NWDAF, which performs inference, derives analytics information (i.e. derives statistics and/or predictions based on Analytics Consumer request) and exposes analytics service i.e. Nnwdaf_AnalyticsSubscription or Nnwdaf_AnalyticsInfo.

- **Model Training logical function (MTLF):** A logical function in NWDAF, which trains Machine Learning (ML) models and exposes new training services (e.g. providing trained ML model) as defined in clause 7.5 and clause 7.6.

NOTE 1: NWDAF can contain an MTLF or an AnLF or both logical functions.

NOTE 2: Pre-trained ML model storage and provisioning to NWDAF is out of the scope of 3GPP.

NOTE 3: In this Release of the specification an NWDAF containing AnLF is locally configured with (a set of) IDs of NWDAFs containing MTLF and the Analytics ID(s) supported by each NWDAF containing MTLF to retrieve trained ML models. An NWDAF containing AnLF uses NWDAF discovery for NWDAF containing MTLF within the set of configured IDs of NWDAFs containing MTLF, if necessary. ML Model provisioning/sharing between multiple MTLFs is not supported in this Release of the specification.

Analytics information are either statistical information of the past events, or predictive information.

Different NWDAF instances may be present in the 5GC, with possible specializations per type of analytics. The capabilities of a NWDAF instance are described in the NWDAF profile stored in the NRF.

To guarantee the accuracy of analytics output for an Analytics ID, based on the UE abnormal behaviour analytics from itself or other NWDAF including abnormal UE list and the observed time window, the NWDAF is to detect and may delete the input data from the abnormal UE(s), and then may generate a new ML model and/or analytics outputs for the Analytics ID without the input data related to abnormal UE list during the observed time window, and then send/update the ML Model Information and/or analytics outputs to the subscribed NWDAF service consumer.

In order to support NFs to discover and select an NWDAF instance containing MTLF, AnLF, or both, that is able to provide the required service (e.g. analytics exposure or ML model provisioning) for the required type of analytics, each NWDAF instance should provide the list of supported Analytics ID(s) (possibly per supported service) when registering to the NRF, in addition to other NRF registration elements of the NF profile. NFs requiring the discovery of an NWDAF instance that provides support for some specific service(s) for a specific type of analytics may query the NRF for NWDAFs supporting the required service(s) and the required Analytics ID(s).

The consumers, i.e. 5GC NFs and OAM, decide how to use the data analytics provided by NWDAF.

The interactions between 5GC NF(s) and the NWDAF take place within a PLMN.

The NWDAF has no knowledge about NF application logic. The NWDAF may use subscription data but only for statistical purpose.

The NWDAF architecture allows for arranging multiple NWDAF instances in a hierarchy/tree with a flexible number of layers/branches. The number and organisation of the hierarchy layers, as well as the capabilities of each NWDAF instance remain deployment choices.

In a hierarchical deployment, NWDAFs may provide data collection exposure capability for generating analytics based on the data collected by other NWDAFs, when DCCF, MFAF are not present in the network.

In order to make NWDAF discoverable in some network deployments, NWDAF may be configured (e.g. for UE mobility analytics) to register in UDM (Nudm_UECM_Registration service operation) for the UE(s) it is serving and for the related Analytics ID(s). Registration in UDM should take place at the time the NWDAF starts serving the UE(s) or collecting data for the UE(s). Deregistration in UDM takes place when NWDAF deletes the analytics context for the UE(s) (see clause 6.1B.4) for a related Analytics ID.

NOTE 4: The procedures for data collection for UE related analytics need to take user consent into account. The user consent for analytics is defined in clause 6.2.9.

5.2 NWDAF Discovery and Selection

The NWDAF service consumer selects an NWDAF that supports requested analytics information and required analytics capabilities and/or requested ML Model Information by using the NWDAF discovery principles defined in clause 6.3.13 ofTS 23.501 [2].

Different deployments may require different discovery and selection parameters. Different ways to perform discovery and selection mechanisms depend on different types of analytics/data (NF related analytics/data and UE related

analytics/data). NF related refers to analytics/data that do not require a SUPI nor group of SUPIs (e.g. NF load analytics). UE related refers to analytics/data that requires SUPI or group of SUPIs (e.g. UE mobility analytics).

In order to discover an NWDAF containing AnLF using the NRF:

- If the analytics is related to NF(s) and the NWDAF service consumer (other than an NWDAF) cannot provide an Area of Interest for the requested data analytics, the NWDAF service consumer may select an NWDAF with large serving area from the candidate NWDAFs from discovery response. Alternatively, in case the consumer receives NWDAF(s) with aggregation capability, the consumer preferably selects an NWDAF with aggregation capability with large serving area.

NOTE 1: If the selected NWDAF cannot provide the requested data analytics, e.g. due to the NF(s) to be contacted being out of serving area of the NWDAF, the selected NWDAF might reject the analytics request/subscription or it might query the NRF with the service area of the NF to be contacted to determine another target NWDAF.

- If the analytics is related to UE(s) and the NWDAF service consumer (other than an NWDAF) cannot provide an Area of Interest for the requested data analytics, the NWDAF service consumer may select an NWDAF with large serving area from the candidate NWDAFs from discovery response. Alternatively, in case the consumer receives NWDAF(s) with aggregation capability, the consumer preferably selects an NWDAF with aggregation capability with large serving area.

NOTE 2: If a selected NWDAF cannot provide analytics for the requested UE(s) (e.g. the NWDAF serves a different serving area), the selected NWDAF might reject the analytics request/subscription or it might determine the AMF serving the UE as specified in clause 6.2.2.1, request UE location information from the AMF, and query the NRF with the tracking area where the UE is located to discover another target NWDAF serving the area where the UE(s) is located.

If the NWDAF service consumer needs to discover an NWDAF that is able to collect data from particular data sources identified by their NF Set IDs or NF types, the consumer may query NRF providing the NF Set IDs or NF types in the discovery request.

NOTE 3: The NF Set ID or NF Type of a data source serving a particular UE, can be determined as indicated in Table 5A.2-1.

In order to discover an NWDAF that has registered in UDM for a given UE:

- NWDAF service consumers or other NWDAFs interested in UE related data or analytics, if supported, may make a query to UDM to discover an NWDAF instance that is already serving the given UE.

If an NWDAF service consumer needs to discover NWDAFs with data collection exposure capability, the NWDAF service consumer may discover via NRF the NWDAF(s) that provide the Nnwdaf_DataManagement service and their associated NF type of data sources or their associated NF Set ID of data sources as defined in clause 6.3.13 of TS 23.501 [2].

In order to discover an NWDAF containing MTLF via NRF:

- an NWDAF containing MTLF shall include the ML model provisioning services (i.e. Nnwdaf_MLModelProvision, Nnwdaf_MLModelInfo) as one of the supported services during the registration in NRF when trained ML models are available for one or more Analytics ID(s). The NWDAF containing MTLF may provide to the NRF a (list of) Analytics ID(s) corresponding to the trained ML models and possibly the ML Model Filter Information for the trained ML model per Analytics ID(s), if available. In this Release of the specification, only the S-NSSAI(s) and Area(s) of Interest from the ML Model Filter Information for the trained ML model per Analytics ID(s) may be registered into the NRF during the NWDAF containing MTLF registration.

NOTE 4: The S-NSSAI(s) and Area(s) of Interest from the ML Model Filter Information are within the indicated S-NSSAI and NWDAF Serving Area information in the NF profile of the NWDAF containing MTLF, respectively.

- During the discovery of NWDAF containing MTLF a consumer (i.e. an NWDAF containing AnLF) may include in the request the target NF type (i.e. NWDAF), the Analytics ID(s), the S-NSSAI(s) and Area(s) of Interest of the Trained ML Model required. The NRF returns one or more candidate for instances of NWDAF containing MTLF to the NF consumer and each candidate for instance of NWDAF containing MTLF includes the Analytics ID(s) and possibly the ML Model Filter Information for the available trained ML models, if available.

NOTE 5: In this Release of the specification, the NWDAF containing AnLF selects from the list of candidate NWDAF (containing MTLF) instance(s), an NWDAF containing MTLF that is pre-configured in the NWDAF containing AnLF to obtain trained ML Model(s) (see clause 5.1).

A PCF may learn which NWDAFs being used by AMF, SMF and UPF for a specific UE, via signalling described in clause 4.16 of TS 23.502 [3]. This enables a PCF to select the same NWDAF instance that is already being used for a specific UE.

5A Data Collection Coordination and Delivery Functional Description

5A.1 General

Data Collection Coordination and Delivery coordinates the collection and distribution of data requested by NF consumers. It prevents data sources from having to handle multiple subscriptions for the same data and send multiple notifications containing the same information due to uncoordinated requests from data consumers.

In this Release of the specification Data Collection Coordination and Delivery is applicable to:

- NWDAFs that request data from a Data Source (e.g. for use in computing analytics).
- NF consumers that request analytics from an NWDAF Data Source.
- NF consumers that request data from an ADRF Data Source.
- ADRFs that receive data from an NF Data Source.

5A.2 Data Collection Coordination

Data Collection Coordination is supported by a DCCF. The Data Consumer may use an NRF to perform NF discovery and selection to find a DCCF that can coordinate data collection (DCCF discovery principles are defined in clause 6.3.19 ofTS 23.501 [2]). Data Consumers send requests for data to the DCCF rather than directly to the NF Data Source. Whether the data consumers directly contact the NF Data Source or goes via the DCCF is based on configuration of the data consumers. For the Data Consumer and each notification endpoint in a data request, the Data Consumer may specify Formatting and Processing Instructions that determine how the data is to be provided. Upon receiving a request from a Data Consumer, the selected DCCF determines the NF instance that can be a Data Source if the Data Source is not indicated in the Data Consumer's request. The DCCF may also select an ADRF if the data is to be stored in an ADRF and an ADRF endpoint is not indicated in the Data Consumer's request. To retrieve data for a specific UE, the NRF, UDM or BSF can provide the DCCF with the identity of the Data Source using the services indicated in table 5A.2-1.

Table 5A.2-1: NF Services consumed by DCCF to determine which NF instances are serving a UE

Type of NF instance (serving the UE) to determine	NF to be contacted by DCCF	Service	Reference in TS 23.502 [3]
UDM	NRF	Nnrf_NFDiscovery	5.2.7.3
AMF	UDM	Nudm_UECM	5.2.3.2
SMF	UDM	Nudm_UECM	5.2.3.2
BSF	NRF	Nnrf_NFDiscovery	5.2.7.3
PCF	BSF	Nbsf_Management	5.2.13.2
NEF	NRF	Nnrf_NFDiscovery	5.2.7.3
NWDAF	UDM	Nudm_UECM	5.2.3.2

The DCCF keeps track of the data actively being collected from the Data Sources it is coordinating. It may do so by maintaining a record of the active prior requests it sends to each Data Source. If a NWDAF subscribes for data directly with a Data Source, or a Data Source has stored data in an ADRF, the NWDAF or ADRF may register the data collection profile with the DCCF.The data collection profile may include the following parameters:

- "Service Operation" identifies the service used to collect the data or analytics from a Data Source (e.g. Namf_EventExposure_Subscribe or Nnwdaf_AnalyticsSubscription_Subscribe);
- "Analytics/Data Specification" is the "Service Operation" specific parameters that identify the collected data (i.e. Analytics ID(s) / Event ID (s), Target of Analytics Reporting or Target of Event Reporting, Analytics Filter or Event Filter, etc.);
- NWDAF ID or ADRF ID specifies the ADRF or NWDAF which registers data collection profile.

The DCCF may then determine certain historical data may be available in the NWDAF or ADRF and coordinate collection of data from the NWDAF or ADRF based on the data collection profile.

When the DCCF receives a request for data, it determines the status of data collection from the Data Source. If parameters in a request for data from a Data Consumer match those in a prior request or in a data collection profile registration, the DCCF may determine that the requested data is already being collected from a Data Source or that a prior subscription to a Data Source may be modified to in addition satisfy the requirements of the new data request from a Data Consumer. This status is used in clause 5A.3 to deliver data to the Data Consumer and notification endpoints.

For persisting event exposure subscriptions for long-lived data collection, the DCCF may subscribe to the UDM to receive event notifications even if a Data Source that serves a UE changes.

The DCCF may subscribe to the NRF to receive event notifications if a Data Source changes (e.g. because of a NF life-cycle event).

NOTE: A DCCF can support multiple Data Sources, Data Consumers, and Message Frameworks. However, to avoid duplicate data collection, each Data Source NF or Set of Data Source NF should be associated with only one DCCF instance or DCCF Set.

A DCCF may use the same mechanisms described in clause 6.2.2.1 to determine AMF and SMF to retrieve data related to "any UE".

If the data consumer requests to collect data for any UE in an area of interest, the data consumer shall first determine all DCCFs covering the area of interest and then contact these DCCFs to request for data collection.

5A.3 Data Delivery

Data is provided to Consumers or notification endpoints according to the Delivery Option configured on the DCCF. Delivery Options are:

1. Delivery via DCCF: Consumers or Notification Endpoints receive the data from the DCCF.
2. Delivery via Messaging Framework: Consumers or Notification Endpoints receive the data from the Messaging Framework via the services offered by the MFAF.

5A.3.1 Data Delivery via the DCCF

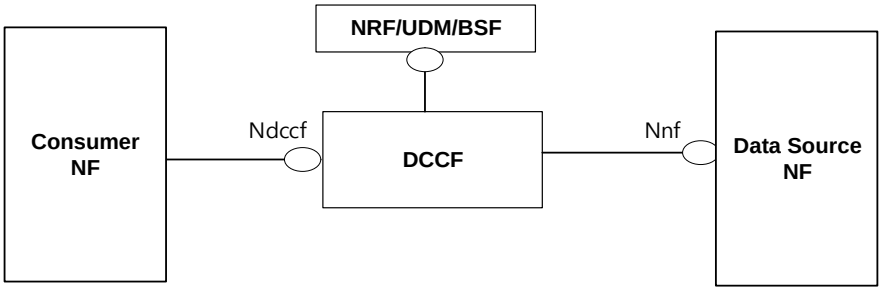

Figure 5A.3.1-1: Data Delivery via DCCF

Data Delivery via DCCF is shown in Figure 5A.3.1-1. Each Event Notification received from a Data Source NF is sent to the DCCF which propagates it to all Data Consumers / Notification Endpoints specified by the Data Consumers or determined by the DCCF. Each Data Consumer may specify in its request to the DCCF multiple notification endpoints, which may include the requesting Data Consumer, an ADRF or other NFs. The DCCF may also select an ADRF or other notification endpoint based on configuration. The DCCF supports formatting and processing for each Consumer / notification endpoint so notifications comply with the data requests received from each Consumer NF.

Upon the DCCF determining the status of data collection for a data request (see clause 5A.2):

- If the requested data is not already being collected from a Data Source, the DCCF sends a new subscription/request towards the Data Source with the notification target specified as the DCCF.
- If the requested data is partially covered by existing subscriptions with the Data Source, the DCCF sends the Data Source a request to modify the subscription.

When notifications are received by the DCCF, they are processed according the Formatting and Processing Instructions for each Consumer and notification endpoint. The DCCF subsequently sends notifications to Consumers and notification endpoints via a Ndccf_DataManagement service.

5A.3.2 Data Delivery via a Messaging Framework

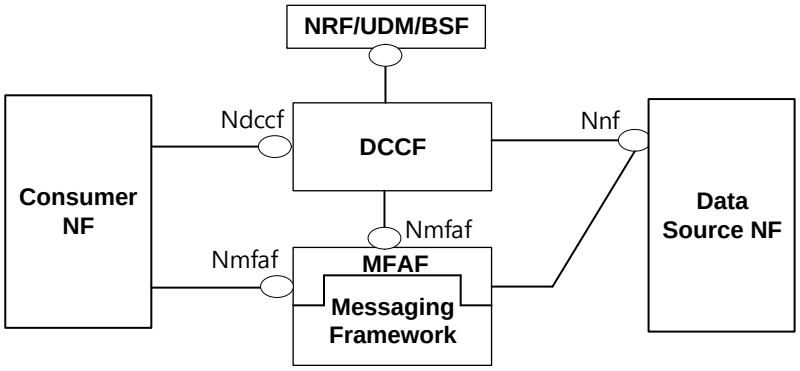

Figure 5A.3.2-1: Data Delivery via a Messaging Framework

Data Delivery via a Messaging Framework is shown in figure 5A.3.2-1. The Messaging Framework formats and processes data received from the Data Source NF and sends notifications to all Data Consumers and Notification Endpoints specified by Data Consumers or determined by the DCCF. Each Data Consumer may specify in its request to the DCCF multiple notification endpoints, which may include the requesting Data Consumer, an ADRF or other NFs. The DCCF may also select an ADRF or other notification endpoint based on configuration. While the Messaging Framework is not standardized by 3GPP, a Messaging Framework Adaptor NF (MFAF) offers 3GPP defined services that allow the 5GS to interact with the Messaging Framework. Internally, the Messaging Framework may for example support the pub-sub pattern, where received data are published to the Messaging Framework and requests from 3GPP Consumers result in Messaging Framework specific subscriptions. Alternatively, the Messaging Framework may support other protocols outside of the scope of 3GPP.

The Messaging Framework Adaptor NF offers services that enable the 5GS to interact with the Messaging Framework:

- 3GPP Consumer Adaptor (3CA) Data Management Service: Nmfaf_3caDataManagement Service delivers data to each Data Consumer or notification endpoint after formatting and processing of data received by the Messaging Framework.

- 3GPP DCCF Adaptor (3DA) Data Management Service: Nmfaf_3daDataManagement Service enables the DCCF to convey to the Messaging Framework, information about the data the Messaging Framework will receive from a Data Source, formatting and processing instructions and the Data Consumer and notification endpoints.

Upon the DCCF determining the status of data collection for a data request (see clause 5A.2):

- If the requested data is not currently being collected from a Data Source, the DCCF sends a new subscription/request towards the Data Source with the notification target specified as the Messaging Framework.

- If the requested data is partially covered by existing subscriptions with the Data Source, the DCCF sends a request to the Data Source to modify one or more subscriptions to accommodate both the previous requests for data and the new request for data.

NOTE: The internal logic of DCCF, e.g. how it decides on what modifications to do, is not specified.

- The DCCF uses the Nmfaf_3daData Management service to convey information so:

  1. the Messaging Framework can recognize data that are received from a Data Source.

  2. the MFAF can obtain data received by the Messaging Framework, process and format the data according to processing and formatting instructions for each Consumer / notification endpoint and send notifications or responses to the Data Consumers.

When data are received by the Messaging Framework (e.g. because of an event notification) they are processed according the Formatting and Processing Instructions for each Consumer / notification endpoint before notifications are sent to the Data Consumer or Notification Endpoints. Notifications sent via the Nmfaf_3caDataManagement service have the same content as those sent via a Ndccf_DataManagement service for Data Delivery via the DCCF.

5A.4 Data Formatting and Processing

Formatting and/or Processing instructions may be provided in requests by Data Consumers via the Ndccf_DataManagement service. When using the Messaging Framework, the DCCF sends the formatting and/or processing instructions to the Messaging Framework via the Nmfaf_3daData_Management Service so the MFAF may format and/or process the data before sending notifications to the Data Consumers / notification endpoints. When using Data Delivery via the DCCF, the DCCF performs formatting and/or processing before sending notifications.

Formatting determines when a notification is sent to the Consumer. Formatting Instructions may indicate:

- Notification Event clubbing: Buffering and sending of several notifications in one message.

- Notification Time Window (example: notifications are buffered and sent between 2 and 3 AM).

- Cross event reference-based notification: When a subscribing NF is subscribing to multiple events (e.g. event X and event Y) the notification for an Event-X is buffered and reported only when the Event-Y occurs.

- Consumer triggered Notification: Notifications are buffered until the consumer requests delivery using Ndccf_DataManagement or Nmfaf_3caDataManagement Service.

NOTE: When this indication is set by the consumer, DCCF or MFAF notifications to the consumer contain Fetch Instructions (see clauses 8.2.4 and 9.3.2).

- Exact time-based Notification: Notifications are sent to the Consumer at an exact time, irrespective of whether the event occurs (example: every 30 min).

- Increasing time window based notification: Notifications are sent to the Consumer at an increasing periodicity (example: the first notification is sent immediately, subsequent received notifications are sent after 5 min, then after 10 min, then after 15 min, etc.).

For an ADRF endpoint, Formatting Instructions sent to the messaging framework may further specify whether Nmfaf services are used to deliver notifications to an ADRF, or whether the data are sent to the ADRF using a Nadrf service.

Processing instructions allow summarizing of notifications to reduce the volume of data reported to the Data Consumer. The processing results in summarizing of information from multiple notifications into a common report. Processing of data for inclusion in each notification sent to consumers occurs over a Processing Interval specified in the Processing Instructions. Notifications sent to consumers may represent partial intervals if formatting instructions or Event Reporting Information (as specified in TS 23.502 [3] table 4.15.1.1-1) require that a notification be sent to the consumer before the end of a processing interval. Processing Instructions are provided per Event ID and are applied to multiple notifications that result from the same subscription and for the same Event ID. Processing Instructions, in addition to the Processing Interval, may specify the parameter names, parameter values and the attributes to be determined and reported to the Consumer. The processed notifications may comprise the following depending on the Event and Processing Instructions:

- Event;

- Processing Interval;

- List of Event Parameter Name(s), and for each Event Parameter Name, one Event Parameter Values and sets of the following attributes as indicated in the processing instructions:

  - Event Spacing: Average and variance of the time interval separating two consecutive occurrences of the same event and parameter value, or periodicity for periodic reporting;

  - Event Duration: Average and variance of the Time for which the parameter value applies;

  - Number of countable occurrences for the parameter (e.g.: Mobility Registration Update);

  - Average and variance of the parameter (e.g.: number of UEs in an AoI);

  - Maximum and minimum parameter values (e.g.: number of UEs in an AoI).

Event Parameter Names are Event specific and not all attributes are applicable for all parameter names. Examples of Event Parameter Names and Parameter values are provided in table 5A.4-1.

Table 5A.4-1: Examples of Event Parameter Names, Parameter values

Event	Event parameter name	Parameter values	Attributes
Location Report	TAI	TAI-7	- Average and variance of the time interval between TA boundary crossings. - Number of TA boundary crossing.
Number of UEs in a Region	Region	AMF-3	- Average and variance of the number of UEs in the Region.
UE Reachability (status change)	CM State	Connected	- Average and variance of time between CM connected state transitions. - Average and variance of the time spent in CM connected state. - Number of transitions to CM connected state.
PDU Session Establishment	DNN	Internet	- Average and variance of time between PDU Session establishments to the Internet DN. - Average and variance of the duration of PDU Sessions established to the Internet DN. - Number of PDUSession establishments to the Internet DN.
PDU Session Establishment	PDU Session Type	Ethernet	- Average and variance of time between Ethernet PDU Session establishments. - Average and variance of the duration of Ethernet PDU Sessions. - Number of Ethernet PDU Session establishments.

5A.5 Historical Data Handling

ADRF or NWDAF as a Data Source:

- When the DCCF receives a request for data that includes a period in the past and ADRF is deployed, the DCCF may obtain data from ADRF as the Data Source. The DCCF may also obtain historical data from an NWDAF. The data obtained from the ADRF or NWDAF is delivered to Consumers / Notification Endpoints according to a configured Delivery Option. The DCCF may determine that requested data may be available in an ADRF or NWDAF based on the data collection profile previously registered by the ADRF or NWDAF, and by querying the ADRF or NWDAF.

ADRF or NWDAF as a Data Recipient:

- An ADRF or NWDAF may be a Consumer NF that initiates requests to the DCCF for data, the ADRF or NWDAF may be specified as a notification endpoint by another Consumer NF that wants to have data it requests archived, or the DCCF may be configured to archive certain data in a ADRF (e.g. all data from an AMF instance).

- If the ADRF or NWDAF instance is not specified in a request for data by a Consumer NF, the DCCF may select the ADRF or NWDAF instance based on provisioned information or information received from the NRF.
- Data is delivered to the ADRF or NWDAF according to a configured Delivery Option (via DCCF or Messaging Framework).

5B Analytics Data Repository Functional Description

5B.1 General

The ADRF offers services that enable a consumer to store and retrieve data and analytics. The analytics are produced by the NWDAF as described in clause 6.1, and data are collected as described in clause 6.2.

Data may be stored in the ADRF by:

- a consumer sending the ADRF an Nadrf_DataManagement_StorageRequest containing the data or analytics to be stored. The ADRF response provides a result indication.
- a consumer sending the ADRF an Nadrf_DataManagement_StorageSubscriptionRequest requesting that the ADRF subscribes to receive data or analytics for storage. The ADRF then subscribes to the NWDAF or DCCF for data or analytics, providing ADRF Notification Address (+Notification Correlation ID). Analytics or Data are subsequently provided as notifications using DCCF, NWDAF or MFAF services (Ndccf_DataManagement Nnwdaf_DataManagement or Nmfaf_3caDataManagement service).

Data may be retrieved from the ADRF by:

- a consumer sending an Nadrf_DataManagement_RetrievalRequest request to the ADRF to retrieve data or analytics for a specified data or analytics collection time window. The ADRF determines the availability of the data or analytics in its repository and sends in the response to the consumer either the data or analytics, or instructions for fetching the data or analytics.
- a consumer sending an Nadrf_DataManagement_RetrievalSubscribe request to the ADRF to retrieve data or analytics for a specified data or analytics collection time window. If the time window includes the future and the ADRF has subscribed to receive the data or analytics, subsequent notifications received by the ADRF are sent by the ADRF to the notification endpoint.

  The ADRF determines the availability of the data or analytics and sends a success/failure indication in the response to the consumer. The ADRF then sends one or more notifications using an Nadrf_DataManagement_RetrievalNotify to the Notification Address (+Notification Correlation ID) specified by the consumer. The notification(s) either provide the data or analytics or provide instructions to the endpoint to fetch the data or analytics using an Nadrf_DataManagement_RetrievalRequest.

Data may be deleted from the ADRF by:

- a consumer sending an Nadrf_DataManagement_Delete request.

An ADRF may be configured to register the data it is collecting with a DCCF. The registration uses the Ndccf_ContextManagement service specified in clause 8.2.3. The registration may subsequently be used by the DCCF to obtain data from the ADRF as described in clause 6.2.6.3.6.

6 Procedures to Support Network Data Analytics

6.0 General

This clause specifies procedures to support network data analytics function.

Clause 6.1 and clause 6.2 specify generic procedures which apply to all type of analytics, while clause 6.3 and onwards specify procedures specific to some type of analytics.

6.1 Procedures for analytics exposure

6.1.1 Analytics Subscribe/Unsubscribe

6.1.1.1 Analytics subscribe/unsubscribe by NWDAF service consumer

This procedure is used by any NWDAF service consumer (e.g. including NFs/OAM) to subscribe/unsubscribe at NWDAF to be notified on analytics information, using Nnwdaf_AnalyticsSubscription service defined in clause 7.2. This service is also used by an NWDAF service consumer to modify existing analytics subscription(s). Any entity can consume this service as defined in clause 7.2.

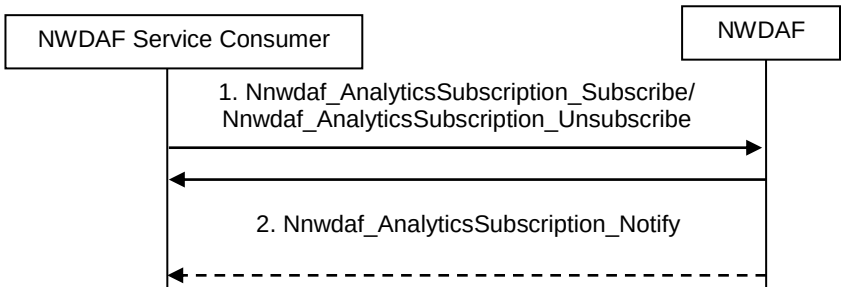

Figure 6.1.1.1-1: Network data analytics Subscribe/unsubscribe

1. The NWDAF service consumer subscribes to or cancels subscription to analytics information by invoking the Nnwdaf_AnalyticsSubscription_Subscribe/ Nnwdaf_AnalyticsSubscription_Unsubscribe service operation. The parameters that can be provided by the NWDAF service consumer are listed in clause 6.1.3.

   When a subscription to analytics information is received, the NWDAF determines whether triggering new data collection is needed.

   If the service invocation is for a subscription modification, the NF service consumer includes an identifier (Subscription Correlation ID) to be modified in the invocation of Nnwdaf_AnalyticsSubscription_Subscribe.

2. If NWDAF service consumer is subscribed to analytics information, the NWDAF notifies the NWDAF service consumer with the analytics information by invoking Nnwdaf_AnalyticsSubscription_Notify service operation, based on the request from the NWDAF service consumer, e.g. Analytics Reporting Parameters. If the NWDAF provides a Termination Request, then the consumer cancels subscription to analytics information by invoking the Nnwdaf_AnalyticsSubscription_Unsubscribe service operation.

6.1.1.2 Analytics subscribe/unsubscribe by AFs via NEF

The analytics exposure to AFs may be performed via NEF by using analytics subscription to NWDAF.

Figure 6.1.1.2-1 illustrates the interaction between AF and NWDAF performed via the NEF.

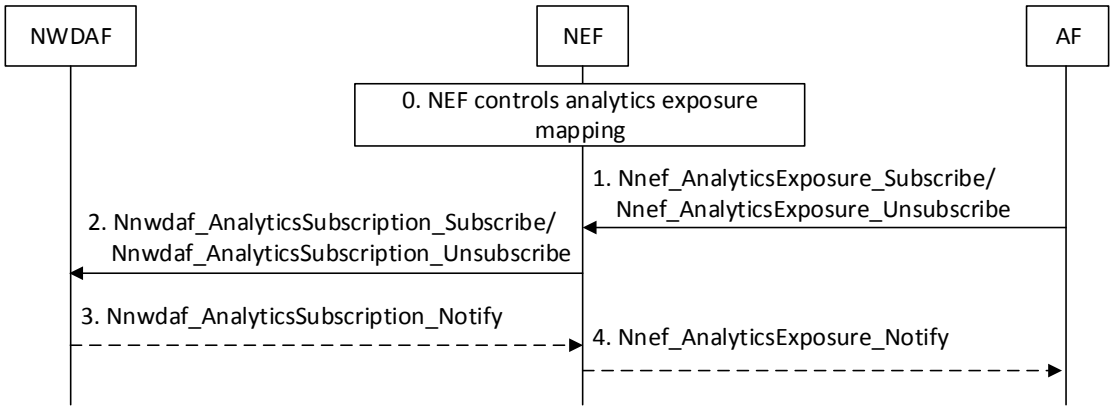

Figure 6.1.1.2-1: Procedure for analytics subscribe/unsubscribe by AFs via NEF

0. NEF controls the analytics exposure mapping among the AF identifier with allowed Analytics ID, and associated inbound restrictions (i.e, applied to subscription of the Analytics ID for an AF) and/or outbound restrictions (i.e. applied to notification of Analytics ID to an AF).

   In this Release, AF is configured with the appropriated NEF to subscribe to analytics information, the allowed Analytics ID(s), and with allowed inbound restrictions (i.e. parameters and/or parameter values) for subscription to each Analytics ID.

1. The AF subscribes to or cancels subscription to analytics information via NEF by invoking the Nnef_AnalyticsExposure_Subscribe/ Nnef_AnalyticsExposure_Unsubscribe service operation defined in TS 23.502 [3]. If the AF wants to modify an existing analytics subscription at NEF, it includes an identifier (Subscription Correlation ID) to be modified in the invocation of Nnef_AnalyticsExposure_Subscribe. If the analytics information subscription is authorized by the NEF, the NEF proceeds with the steps below.

2. Based on the request from the AF, the NEF subscribes to or cancels subscription to analytics information by invoking the Nnwdaf_AnalyticsSubscription_Subscribe/ Nnwdaf_AnalyticsSubscription_Unsubscribe service operation.

   If the parameters and/or parameters values of the AF request comply with the inbound restriction in the analytics exposure mapping, NEF forwards in the subscription to NWDAF service the Analytics ID, parameters and/or parameters values from the AF request.

   If the request from AF does not comply with the restrictions in the analytics exposure mapping, NEF may apply restrictions to the subscription request to NWDAF (e.g. restrictions to parameters or parameter values of the Nnwdaf_AnalyticsSubscription_Subscribe service operations), based on operator configuration and/or may apply parameter mapping (e.g. geo coordinate mapping to TA(s)/Cell-id(s)).

   The NEF records the association of the analytics request from the AF and the analytics request sent to the NWDAF.

   The NEF selects an NWDAF that supports analytics information requested by the AF using the NWDAF discovery procedure defined in TS 23.501 [2].

   If the AF request is for a modification of the existing analytics subscription(s), the NEF invokes Nnwdaf_AnalyticsSubscription_Subscribe to modify the analytics subscription identified by an identifier (Subscription Correlation ID) associated with the AF.

3. If the NEFhas subscribed to analytics information, the NWDAF notifies the NEF with the analytics information or Termination Request by invoking Nnwdaf_AnalyticsSubscription_Notify service operation.

4. If the NEF receives the notification from the NWDAF, the NEF notifies the AF with the analytics information or Termination Request by invoking Nnef_AnalyticsExposure_Notify service operation defined in TS 23.502 [3]. NEF may apply outbound restrictions to the notifications to AFs (e.g. restrictions to parameters or parameter values of the Nnef_AnalyticsExposure_Notify service operation) based on analytics exposure mapping and may

apply parameter mapping for external usage (e.g. TA(s), Cell-id(s) to geo coordinate). The AF checks if a Termination Request is present in the Nnef_AnalyticsExposure_Notify as defined in step 2 in clause 6.1.1.1.

6.1.2 Analytics Request

6.1.2.1 Analytics request by NWDAF service consumer

This procedure is used by the NWDAF service consumer (e.g. including NFs/OAM) to request and get from NWDAF analytics information, using Nnwdaf_AnalyticsInfo service defined in clause 7.3.

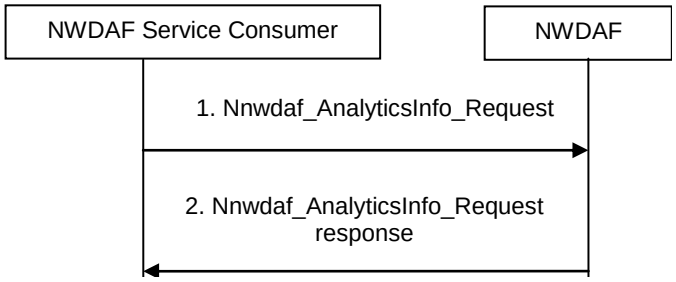

Figure 6.1.2.1-1: Network data analytics Request

1. The NWDAF service consumer requests analytics information by invoking Nnwdaf_AnalyticsInfo_Request service operation. The parameters that can be provided by the NWDAF service consumer are listed in clause 6.1.3.

   When a request for analytics information is received, the NWDAF determines whether triggering new data collection is needed.

2. The NWDAF responds with analytics information to the NWDAF service consumer. The NWDAF checks if a Termination Request is indicated as defined in step 2 in clause 6.1.1.1.

6.1.2.2 Analytics request by AFs via NEF

The analytics exposure to AFs may be performed via NEF by using analytics request to NWDAF.

Figure 6.1.2.2-1 illustrates the interaction between AF and NWDAF performed via the NEF.

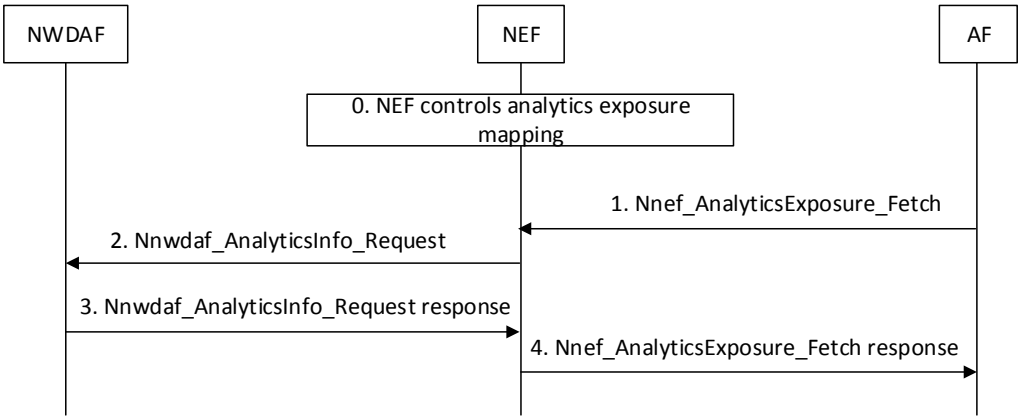

Figure 6.1.2.2-1: Procedure for analytics request by AFs via NEF

0. NEF controls the analytics exposure mapping among the AF identifier with allowed Analytics ID(s), and associated inbound restrictions (i.e. applied to the Analytics ID requested by AF, and/or outbound restrictions (i.e. applied to the response of Analytics ID to AF).

In this Release, AF is configured, e.g. via static OAM configuration, with the appropriated NEF to subscribe to analytics information, the allowed Analytics ID(s), and with allowed inbound restrictions (i.e. parameters and/or parameter values) for requesting each Analytics ID.

1. The AF requests to receive analytics information via NEF by invoking the Nnef_AnalyticsExposure_Fetch service operation defined in TS 23.502 [3]. If the analytics information request is authorized by the NEF, the NEF proceeds with the steps below.

2. Based on the request from the AF, the NEF requests analytics information by invoking the Nnwdaf_AnalyticsInfo_Request service operation.

   If the parameters and/or parameters values of the AF request comply with the restriction in the analytics exposure mapping, NEF forwards in the subscription to NWDAF service the Analytics ID, parameters and/or parameters values from AF in the request to NWDAF.

   If the request from AF does not comply with the restrictions in the analytics exposure mapping, NEF may apply restrictions to the request to NWDAF (e.g. restrictions to parameters or parameter values of the Nnwdaf_AnalyticsInfo_Request service operations) based on operator configuration and/or may apply parameter mapping (e.g. geo coordinate mapping to TA(s), Cell-id(s)).

   The NEF records the association of the analytics request from the AF and the analytics request sent to the NWDAF.

   The NEF selects an NWDAF that supports analytics information requested by the AF using the NWDAF discovery procedure defined in TS 23.501 [2].

3. The NWDAF responds with the analytics information to the NEF.

4. The NEF responds with the analytics information to the AF. NEF may apply restrictions to the response to AFs (e.g. restrictions to parameters or parameter values of the Nnef_AnalyticsExposure_Fetch response service operation) based on operator configuration. The AF checks if a Termination Request is present and then follows as defined in step 2 in clause 6.1.1.1.

6.1.3 Contents of Analytics Exposure

The consumers of the Nnwdaf_AnalyticsSubscription_Subscribe or Nnwdaf_AnalyticsInfo_Request service operations described in clause 7 provide the following input parameters listed below.

- A list of Analytics ID(s): identifies the requested analytics.
  - Analytics Filter Information: indicates the conditions to be fulfilled for reporting Analytics Information. This set of optional parameter types and values enables to select which type of analytics information is requested. Analytics Filter Information is defined in the analytics related clauses.
- Target of Analytics Reporting: indicates the object(s) for which Analytics information is requested, entities such as specific UEs, a group of UE(s) or any UE (i.e. all UEs).
- (Only for Nnwdaf_AnalyticsSubscription_Subscribe) A Notification Target Address (+ Notification Correlation ID) as defined in TS 23.502 [3] clause 4.15.1, allowing to correlate notifications received from NWDAF with this subscription.
- (Only for Nnwdaf_AnalyticsSubscription_Subscribe) Subscription Correlation ID: identifies an existing analytics subscription that is to be modified.
- Related to analytic consumers that aggregate analytics from multiple NWDAF subscriptions:
  - [OPTIONAL] (Set of) NWDAF identifiers of NWDAF instances used by the NWDAF service consumer when aggregating multiple analytics subscriptions. See clause 6.1A.
- Analytics Reporting Information with the following parameters:
  - (Only for Nnwdaf_AnalyticsSubscription_Subscribe) Analytics Reporting Parameters as per Event Reporting parameters defined in Table 4.15.1-1 ofTS 23.502 [3].

NOTE 1: When the Analytics Reporting Parameters indicates a periodic reporting mode and the periodicity of the report is equal to or greater than the Supported Analytics Delay associated with the Analytics ID (if available) defined in clause 6.2.6.2 of TS 23.501 [2], it is expected that the periodic reporting can be provided by the NWDAF as requested.

- (Only for Nnwdaf_AnalyticsSubscription_Subscribe) Reporting Thresholds, which indicate conditions on the level of each requested analytics that when reached shall be notified by the NWDAF.
  - [OPTIONAL] Matching direction: A matching direction may be provided such as below, above, or crossed. If no matching direction is provided, the default direction is crossed.
  - [OPTIONAL] Acceptable deviation: An acceptable deviation from the threshold level in the non-critical direction (i.e. in which the QoS is improving) may be set to limit the amount of signalling.
- Analytics target period: time interval [start..end], either in the past (both start time and end time in the past) or in the future (both start time and end time in the future). An Analytics target period in the past is a request or subscription for statistics. An Analytics target period in the future is a request or subscription for predictions. The time interval is expressed with actual start time and actual end time (e.g. via UTC time). When the Analytics Reporting Parameters indicate a periodic reporting mode, the time interval can also be expressed as positive or negative offsets to the reporting time, which indicates a subscription for predictions or statistics respectively. By setting start time and end time to the same value, the consumer of the analytics can request analytics or subscribe to analytics for a specific time rather than for a time interval.
- [OPTIONAL] Data time window: if specified, only events that have been created in the specified time interval are considered for the analytics generation.
- [OPTIONAL] Preferred level of accuracy of the analytics ("Low", "Medium", "High" or "Highest").
- [OPTIONAL] Preferred level of accuracy per analytics subset ("Low", "Medium", "High" or "Highest"). When a preferred level of accuracy is expressed for a given analytics subset, it takes precedence for this subset over the above preferred level of accuracy of the analytics. Analytics subsets are defined in the "Output Analytics" clause of applicable analytics.
- [OPTIONAL] Dataset Statistical Properties: information in order to influence the data selection mechanisms to be used for the generation of an Analytics ID, assuring that the generated Analytics ID reflects the statistical characteristics of the data that are relevant for the NWDAF consumer. The following dataset statistical properties are allowed:
  - Uniformly distributed datasets, which indicates the use of data samples that are uniformly distributed according to the different aspects of the requested analytics (e.g. equivalent data samples for each UE listed as a Target of Analytics Reporting or for S-NSSAIs included in the Analytics Filter Information).
  - Datasets with or without outliers, which indicates that the data samples shall consider or disregard data samples that are at the extreme boundaries of the value range.
- Time when analytics information is needed (if applicable): indicates to the NWDAF the latest time the analytics consumer expects to receive analytics data provided by the NWDAF. It should not be set to a value less than the Supported Analytics Delay of the selected NWDAF if applicable. If the time is reached the consumer does not need to wait for the analytics information any longer, yet the NWDAF may send an error response or error notification to the consumer. "Time when analytics information is needed" is a relative time interval as the gap with respect to analytics request /subscription (e.g. "in 10 minutes").

NOTE 2: If the analytics request contains the parameter "Time when analytics information is needed" for Analytics ID(s), this parameter takes precedence over the requested periodicity, if a periodic reporting mode is requested.

NOTE 3: If the Time when analytics information is needed is provided and it is less than the Supported Analytics Delay per Analytics ID (if available) defined in clause 6.2.6.2 of TS 23.501 [2], it is expected that the NWDAF might not be able to treat the Analytics ID on time.

- [OPTIONAL] Maximum number of objects requested by the consumer (max) to limit the number of objects in a list of analytics per Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response.
- [OPTIONAL] Preferred granularity of location information: TA level or cell level.

- [OPTIONAL] Preferred order of results when a list of analytics is returned, possibly with a criterion for identifying the property of the results to which the preferred ordering is applied.

- [OPTIONAL] Maximum number of SUPIs (SUPImax) requested by the consumer to limit the number of SUPIs in an object. When SUPImax is not provided, the NWDAF shall return all SUPIs concerned by the analytics object. When SUPImax is set to 0, the NWDAF shall not provide any SUPI.

- [OPTIONAL] Output strategy: indicates the relevant factors for determining when the analytics reported. The following values are allowed:

  - Binary output strategy: indicates that the analytics shall only be reported when the preferred level of accuracy is reached within a cycle of periodic notification as defined in the Analytics Reporting Parameters.

NOTE 4: If preferred level of accuracy is more important than providing an output, then the binary strategy is used so that all analytics outputs have equivalent confidence in the prediction.

  - Gradient output strategy: indicates that the analytics shall be reported according with the periodicity defined in the Analytics Reporting Parameters irrespective if the preferred level of accuracy has been reached.

NOTE 5: If having an analytics output is more important than reaching the preferred level of accuracy, then the gradient output strategy is used so that each NWDAF will timely provide the output indicating the confidence of the prediction at the moment of the output generation.

NOTE 6: When no output strategy is included in the subscription, the analytics output will be generated based on the gradient strategy and includes the confidence of the prediction for the reporting period.

- [OPTIONAL] Analytics metadata request: indicates a request from one NWDAF to another NWDAF to provide the "analytics metadata information" related to the produced output analytics. This input parameter indicates which parameters in "analytics metadata information" are required to aggregate the output analytics for the requested Analytics ID(s).

- (Only for Nnwdaf_AnalyticsSubscription_Subscribe) Consumer NF's serving area or NF ID. During a pending analytics subscription transfer, this information can be used by the NWDAF to find out if the analytics consumers may change as described in clause 6.1B.2.

- (Only for Nnwdaf_AnalyticsSubscription_Subscribe) Information of previous analytics subscription. When setting up the analytics generation, this information may be used to retrieve analytics context from the previous NWDAF in order to build upon the context that is already related to this subscription as described in clause 6.1B.2.1.

The NWDAF provides to the consumer of the Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request service operations described in clause 7, the output information listed below:

- (Only for Nnwdaf_AnalyticsSubscription_Notify) The Notification Correlation Information.

- For each Analytics ID the analytics information in the requested Analytics target period.

- Timestamp of analytics generation: allows consumers to decide until when the received information shall be used. For instance, an NF can deem a received notification from NWDAF for a given feedback as invalid based on this timestamp;

- Validity period: defines the time period for which the analytics information is valid.

- Confidence: probability assertion:, i.e. confidence in the prediction.

- [OPTIONAL] For each Analytics ID the Termination Request, which notifies the consumer that the subscription is requested to be cancelled as the NWDAF can no longer serve this subscription, e.g. due to user consent revoked, NWDAF overload, UE moved out of NWDAF serving area, etc.

- [OPTIONAL] Analytics metadata information: additional information required to aggregate the output analytics for the requested Analytics ID(s). This parameter shall be provided if the "Analytics metadata request" parameter was provided in the corresponding Nnwdaf_AnalyticsSubscription_Subscribe or Nnwdaf_AnalyticsInfo_Request service operation.

- Number of data samples used for the generation of the output analytics;
- Data time window of the data samples;
- Dataset Statistical Properties of the analytics output used for the generation of the analytics;
- [OPTIONAL] Data source(s) of the data used for the generation of the output analytics;
- [OPTIONAL] Data Formatting and Processing applied on the data;
- Output strategy used for the reporting of the analytics.

- (Only for error response or error notification) Revised waiting time: indicates to the consumer a revised waiting value for "Time when analytics information is needed". Each NWDAF may include this as part of error response or error notification to "Time when analytics information is needed" as described in clause 6.2.5. Revised waiting time is the minimum time interval recommended by NWDAF to use as "Time when analytics information is needed" for similar future analytics requests/subscriptions.

6.1.4 Analytics Exposure using DCCF

6.1.4.1 General

This clause specifies procedures for analytics exposure using DCCF services, with two options: analytics can be exposed via DCCF, according to clauses 6.1.4.2 and 6.1.4.3, or can be exposed via a messaging framework according to clauses 6.1.4.4 and 6.1.4.5. Which option to use is determined by DCCF configuration.

6.1.4.2 Analytics Exposure via DCCF

The procedure as depicted in Figure 6.1.4.2-1 is used by analytics consumer(s) (e.g. NFs/OAM) to subscribe/unsubscribe to NWDAF analytics and be notified of analytics information via the DCCF, using Ndccf_DataManagement_Subscribe service operation. Whether a NWDAF service consumer directly contacts the NWDAF or goes via the DCCF is based on NWDAF service consumer configuration.

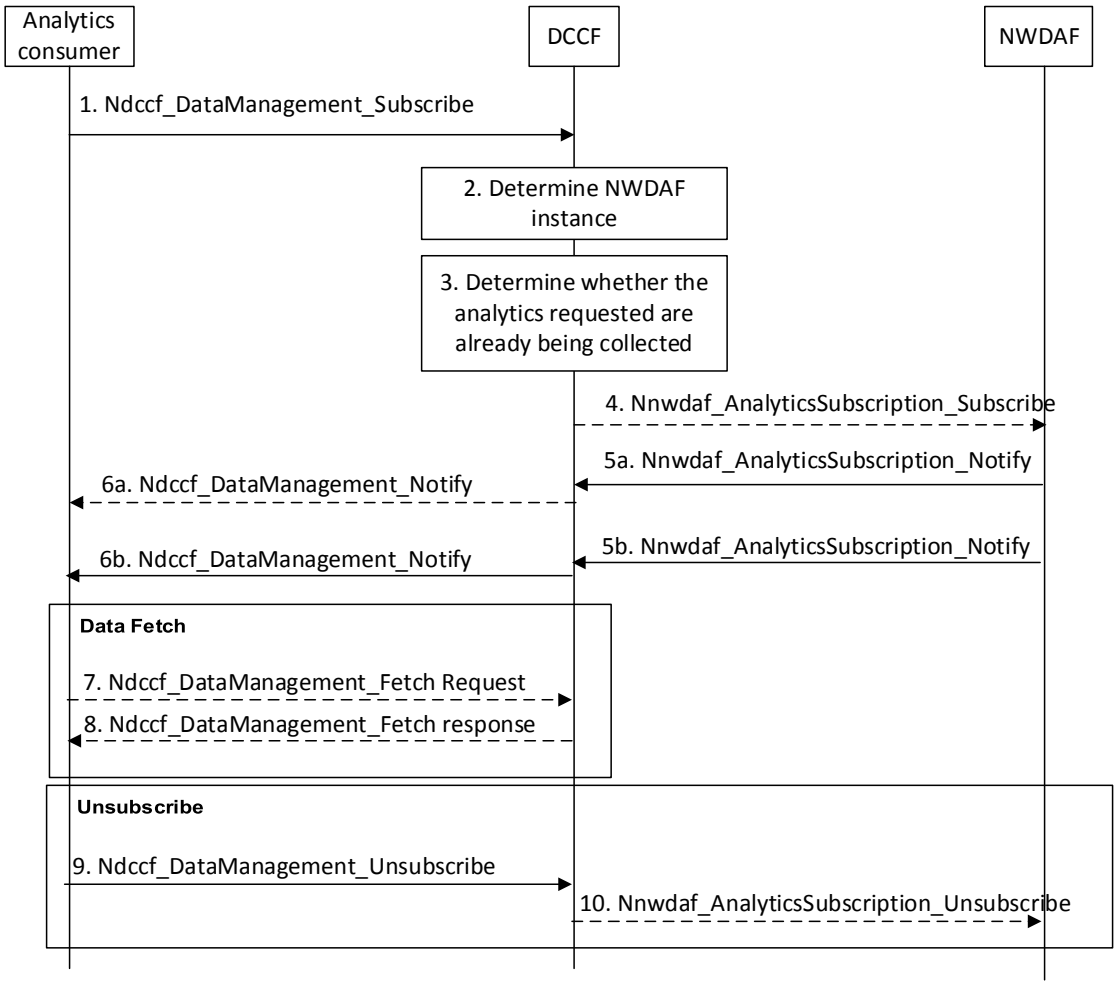

Figure 6.1.4.2-1: Network data analytics subscription via DCCF

1. Analytics consumer subscribes to analytics information via DCCF by invoking the Ndccf_DataManagement_Subscribe(Nnwdaf service operation, Analytics Specification, Formatting Instructions, Processing Instructions, NWDAF (or NWDAF-Set) ID, ADRF Information) service operation. The analytics consumer may specify one or more notification endpoints. Analytics consumer decides to go via DCCF based on internal configuration. The "Analytics Specification" provides Nnwdaf service operation specific parameters, e.g. Analytics IDs, Target of Analytics Reporting, and optional parameters used to retrieve the analytics. The analytics consumer may provide the identity of the NWDAF to collect analytics from. The analytics consumer may provide additional information on possible notification endpoints or ADRF information so analytics are archived.

2. If the NWDAF instance or NWDAF Set is not identified by the analytics Consumer, the DCCF determines the NWDAF instances that can provide analytics. If the consumer requested storage of analytics in an ADRF but an ADRF ID is not provided by the Analytics Consumer, or the collected analytics is to be stored in an ADRF according to configuration on the DCCF, the DCCF selects an ADRF to store the collected data.

3. The DCCF determines whether the analytics requested in step 1 are already being collected. If the requested analytics are already being collected by an Analytics Consumer, the DCCF adds the new analytics consumer to the list of analytics consumers that are subscribed for these analytics.

4. If the analytics subscribed in step 1 partially matches an analytics that is already being collected by the DCCF from an NWDAF, and a modification of this subscription to the NWDAF would satisfy both the existing analytics subscriptions as well as the newly requested analytics, the DCCF invokes a modification of the previous subscription via Nnwdaf_AnalyticsSubscription_Subscribe service operation (as specified in clause 6.1.1.1), and the DCCF adds the analytics consumer to the list of analytics consumers that are subscribed for these analytics.

If the analytics requested at step 1 are not already available or not being collected yet, the DCCF subscribes to analytics from NWDAF using the Nnwdaf_AnalyticsSubscription_Subscribe procedure as specified in clause 6.1.1.1. The DCCF adds the analytics consumer to the list of analytics consumers that are subscribed for these analytics.

5. When new output analytics are available, the NWDAF notifies the analytics information to the DCCF by invoking Nnwdaf_AnalyticsSubscription_Notify service operation.

6. The DCCF uses Ndccf_DataManagement_Notify to send the analytics to all notification endpoints indicated in step 1. Analytics sent to notification endpoints may be processed and formatted by the DCCF so they conform to delivery requirements for each analytics consumer or notification endpoint as specified in clause 5A.4. The DCCF may store the analytics in the ADRF if requested by the consumer or if required by DCCF configuration, using procedure as specified in clause 6.2B.3.

NOTE: According to Formatting Instructions provided by the Analytics Consumer, multiple notifications from a NWDAF can be combined in a single Ndccf_DataManagement_Notify so many notifications from an NWDAF results in fewer notifications (or one notification) to the Analytics Consumer. Alternatively, a notification can instruct the analytics notification endpoint to fetch the analytics from the DCCF.

7. If a Ndccf_DataManagement_Notify contains a fetch instruction, the notification endpoint sends a Ndccf_DataManagement_Fetch request to fetch the analytics from the DCCF before an expiry time.

8. The DCCF delivers the analytics to the notification endpoint.

9. When the Analytics Consumer no longer wants analytics to be collected it invokes Ndccf_DataManagement_Unsubscribe(Subscription Correlation ID), using the Subscription Correlation Id received in response to its subscription in step 1. The DCCF removes the analytics consumer from the list of analytics consumers that are subscribed for these analytics.

10. If there are no other Analytics Consumers subscribed to the analytics, the DCCF unsubscribes with the NWDAF.

6.1.4.3 Historical Analytics Exposure via DCCF

The procedure as depicted in Figure 6.1.4.3-1 is used by an analytics consumer (e.g. NFs/OAM) to obtain historical analytics via the DCCF. Historical analytics may be previously computed statistics or predictions stored in an NWDAF or ADRF. Statistics may have been previously computed and stored in the ADRF or NWDAF and can be identified by a "target period" in the past (see clause 6.1.3). Requests for previously computed predictions have a "Time Window", which specifies an allowable span for when the predictions may have been computed. This allows the Analytics Consumer to request previously computed predictions for a target period.

The analytics consumer requests analytics via the DCCF, using Ndccf_DataManagement_Subscribe service operation. Whether the NWDAF service consumer directly contacts the NWDAF/ADRF or goes via the DCCF is based on configuration.

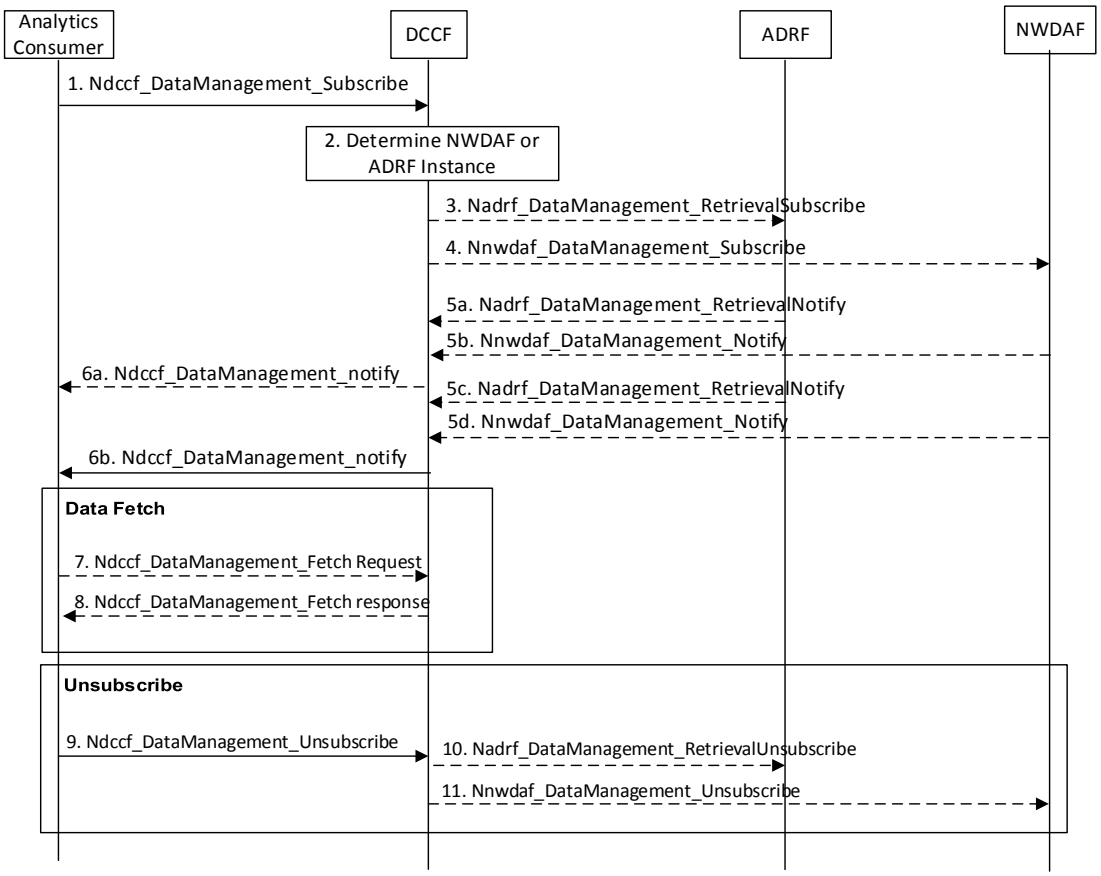

Figure 6.1.4.3-1: Historical Analytics Exposure via DCCF

1. The analytics consumer requests analytics via DCCF by invoking the Ndccf_DataManagement_Subscribe(Nnwdaf service operation, Analytics Specification, Time Window, Formatting Instructions, Processing Instructions, ADRF ID or NWDAF ID (or ADRF Set ID or NWDAF Set ID) service operation as specified in clause 8.2.2. The analytics consumer may specify one or more notification endpoints to receive the analytics.

Parameter "Nnwdaf service operation" is the service operation used to originally acquire the analytics and identifies this as a request for analytics, "Analytics Specification" provides Nnwdaf service operation specific parameters, e.g. Analytics IDs, Target of Analytics Reporting, and optional parameters used to retrieve the analytics. "Time Window" specifies a past time period and comprises a start and stop time indicating when predictions were computed, and "Formatting and Processing Instructions" are as defined in clause 5A.4. The analytics consumer may optionally include the ADRF or NWDAF instance (or ADRF Set or NWDAF Set) ID where the stored analytics resides.

2. If an ADRF or NWDAF instance or ADRF or NWDAF Set ID is not provided by the analytics consumer, the DCCF determines if any ADRF or NWDAF instances might provide the analytics as described in clause 5A and clause 5B.

3. (conditional) If the DCCF determines that an ADRF instance might provide the analytics, or an ADRF instance or Set was supplied by the analytics consumer, the DCCF sends a request to the ADRF, using Nadrf_DataManagement_RetrievalSubscribe(Analytics Specification, Notification Target Address=DCCF) service operation, as specified in clause 10.2. The ADRF responds to the DCCF with an Nadrf_DataManagement_RetrievalSubscribe response indicating if the ADRF can supply the analytics. If the analytics can be provided, the procedure continues with step 5.

4. (conditional) If the DCCF determines that an NWDAF instance might provide the analytics or an NWDAF instance or Set was supplied by the Analytics Consumer, the DCCF sends a request to the NWDAF using Nnwdaf_DataManagement_Subscribe(Analytics Specification, Notification Target Address=DCCF) as specified in clause 7.4.2.

5. The ADRF uses Nadrf_DataManagement_RetrievalNotify or the NWDAF uses Nnwdaf_DataManagement_Notify to send the requested analytics (e.g. one or more stored notifications archived from an NWDAF) to the DCCF. The analytics may be sent in one or more notification messages.

6. The DCCF uses Ndccf_DataManagement_Notify to send analytics to all notification endpoints indicated in step 1. Notifications are sent to the Notification Target Address(es) using the Analytics Consumer Notification Correlation ID(s) received in step 1. Analytics sent to notification endpoints may be processed and formatted by the DCCF, so they conform to delivery requirements specified by the analytics consumer.

NOTE: According to Formatting Instructions provided by the analytics consumer, multiple notifications from an ADRF or NWDAF can be combined in a single Ndccf_DataManagement_Notify so many notifications from the ADRF or NWDAF results in fewer notifications (or one notification) to the Analytics Consumer. Alternatively, a Ndccf_DataManagement_Notify can instruct the analytics notification endpoint to fetch the analytics from the DCCF before an expiry time.

7. If a notification contains a fetch instruction, the notification endpoint sends a Ndccf_DataManagement_Fetch request as specified in clause 8.2.5 to fetch the analytics from the DCCF.

8. The DCCF delivers the analytics to the notification endpoint.

9. When the analytics consumer no longer wants analytics to be collected or has received all the analytics it needs, it invokes Ndccf_DataManagement_Unsubscribe(Subscription Correlation ID), using the Subscription Correlation Id received in response to its subscription in step 1.

10. If the analytics are being provided by an ADRF and there are no other analytics consumers subscribed to the analytics, the DCCF unsubscribes with the ADRF using Nadrf_DataManagement_RetrievalUnsubscribe as specified in clause 10.2.7.

11. If the analytics are being provided by an NWDAF and there are no other analytics consumers subscribed to the analytics, the DCCF unsubscribes with the NWDAF using Nnwdaf_DataManagement_Unsubscribe service operation as specified in clause 7.4.3.

6.1.4.4 Analytics Exposure via Messaging Framework

The procedure as depicted in Figure 6.1.4.4-1 is used by analytics consumer(s) (e.g. NFs/OAM) to subscribe/unsubscribe to NWDAF analytics and be notified of analytics information, using Ndccf_DataManagement_Subscribe service operation. The 3GPP DCCF Adaptor (3da) Data Management service and 3GPP Consumer Adaptor (3ca) Data Management service of the Messaging Framework Adaptor Function (MFAF) are used to interact with the 3GPP Network and the Messaging Framework. Whether a NWDAF service consumer directly contacts the NWDAF or goes via the DCCF is based on NWDAF service consumer configuration.

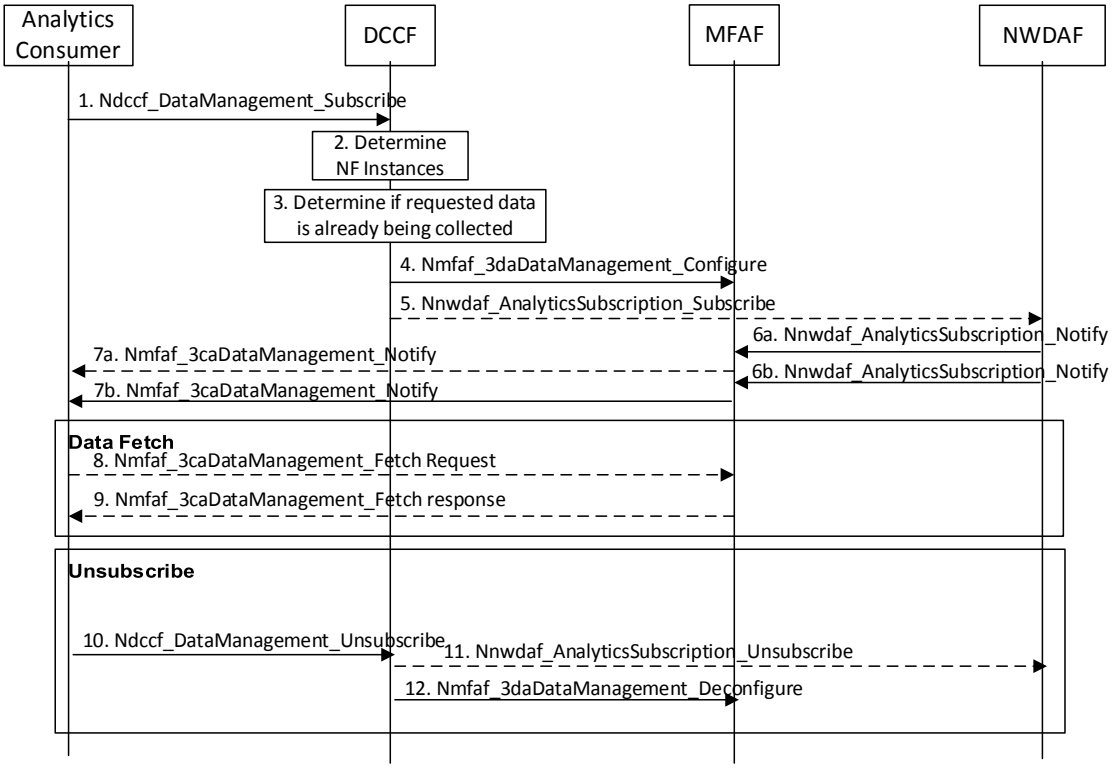

Figure 6.1.4.4-1: Network data analytics subscription via DCCF

1. Analytics consumer subscribes to analytics information via DCCF by invoking the Ndccf_DataManagement_Subscribe (Nnwdaf service operation, Analytics Specification, Formatting Instructions, Processing Instructions, NWDAF (or NWDAF-Set) ID, ADRF Information, Analytics Consumer Notification Target Address (+ Notification Correlation ID)) service operation. The analytics consumer may specify one or more notification endpoints. Analytics consumer decides to go via DCCF based on internal configuration. The "Analytics Specification" provides Nnwdaf service operation specific parameters, e.g. Analytics IDs, Target of Analytics Reporting, and optional parameters used to retrieve the analytics. The analytics consumer may provide the identity of the NWDAF to collect analytics from. The analytics consumer may provide additional information on possible notification endpoints or ADRF information to archive analytics.

2. If the NWDAF instance or NWDAF Set is not identified by the analytics consumer, the DCCF determines the NWDAF instances that can provide analytics. If the consumer requested storage of analytics in an ADRF but an ADRF ID is not provided by the Analytics Consumer, or the collected analytics is to be stored in an ADRF according to configuration on the DCCF, the DCCF selects an ADRF to store the collected analytics.

3. The DCCF determines whether the analytics requested in step 1 are already being collected. If the requested analytics are already being collected by an analytics consumer, the DCCF adds the new analytics consumer to the list of analytics consumers that are subscribed for these analytics.

4. The DCCF sends an Nmfaf_3daDataManagement_Configure(Analytics Consumer Information, MFAF Notification Information, Formatting Conditions, Processing Instructions) to configure the MFAF to map notifications received from the NWDAF to outgoing notifications sent to endpoints, and to instruct the MFAF how to format and process the outgoing notifications.

   "Analytics Consumer Information" contains for each notification endpoint, the analytics consumer Notification Target Address (+ Analytics Consumer Notification Correlation ID) to be used by the MFAF when sending notifications in step 7.

   "MFAF Notification Information" is included if an NWDAF is already sending the analytics to the MFAF. MFAF Notification Information identifies Event Notifications received from the NWDAF and comprises the MFAF Notification Target Address (+ MFAF Notification Correlation ID). If the MFAF does not receive MFAF Notification information from the DCCF, the MFAF selects an MFAF Notification Target Address (+ MFAF Notification Correlation ID) and sends the MFAF Notification Information, containing the MFAF Notification

Target Address (+ MFAF Notification Correlation ID), to the DCCF in the Nmfaf_3daDataManagement_Configure Response.

5. If the analytics subscribed in step 1 partially matches analytics that are already being collected by the DCCF from a NWDAF, and a modification of this subscription to the NWDAF would satisfy both the existing analytics subscriptions as well as the newly requested analytics, the DCCF invokes Nnwdaf_AnalyticsSubscription_Subscribe(Subscription Correlation ID) with parameters indicating how to modify the previous subscription (as specified in clause 6.1.1.1). The DCCF adds the analytics consumer to the list of analytics consumers that are subscribed for these analytics.

   If the analytics requested at step 1 are not already available or not being collected yet, the DCCF subscribes to analytics from the NF using Nnwdaf_AnalyticsSubscription_Subscribe, setting the Notification Target Address (+Notification Correlation ID)) to the MFAF Notification Target Address (+ MFAF Notification Correlation ID) received in step 4. The DCCF adds the analytics consumer to the list of analytics consumers that are subscribed for these analytics.

6. When new output analytics are available, the NWDAF uses Nnwdaf_AnalyticsSubscription_Notify to send the analytics to the MFAF. The Notification includes the MFAF Notification Correlation ID.

7. The MFAF uses Nmfaf_3caDataManagement_Notify to send the analytic to all notification endpoints indicated in step 4. Notifications are sent to the Notification Target Address(es) using the Analytics Consumer Notification Correlation ID(s) received in step 4. Analytics sent to notification endpoints may be processed and formatted by the MFAF, so they conform to delivery requirements specified by the analytics consumer. The MFAF may store the information in the ADRF if requested by consumer or if required by DCCF configuration, using procedure as specified in clause 6.2B.3.

NOTE: According to Formatting Instructions provided by the Analytics Consumer, multiple notifications from a NWDAF can be combined in a single Nmfaf_3caDataManagement_Notify, so many notifications from the NWDAF results in fewer notifications (or one notification) to the analytics consumer. Alternatively, a notification can instruct the analytics notification endpoint to fetch the analytics from the MFAF before an expiry time.

8. If a Nmfaf_3caDataManagement_Notify contains a fetch instruction, the notification endpoint sends a Nmfaf_3caDataManagement_Fetch request to fetch the analytics from the MFAF.

9. The MFAF delivers the analytics to the notification endpoint.

10. When the analytics consumer no longer wants analytics to be collected, it invokes Ndccf_DataManagement_Unsubscribe(Subscription Correlation ID), using the Subscription Correlation Id received in response to its subscription in step 1. The DCCF removes the analytics consumer from the list of analytics consumers that are subscribed for these analytics.

11. If there are no other analytics consumers subscribed to the analytics, the DCCF unsubscribes with the NWDAF.

12. The DCCF de-configures the MFAF so it no longer maps notifications received from the NWDAF to the notification endpoints configured in step 4.

6.1.4.5 Historical Analytics Exposure via Messaging Framework

The procedure as depicted in Figure 6.1.4.5-1 is used by an analytics consumer (e.g. NFs/OAM) to obtain historical analytics via the messaging framework. Historical analytics may be previously computed statistics or predictions stored in an NWDAF or ADRF. Statistics may be previously computed and stored in the ADRF or NWDAF and can be identified by a "target period" in the past (see clause 6.1.3). Requests for previously computed predictions have a "Time Window", which specifies an allowable span for when the predictions may have been computed. This allows the analytics consumer to request previously computed predictions for a target period.

The analytics consumer requests analytics via the DCCF, using Ndccf_DataManagement_Request service operation. Whether the NWDAF service consumer directly contacts the NWDAF/ADRF, or goes via the DCCF is based on configuration.

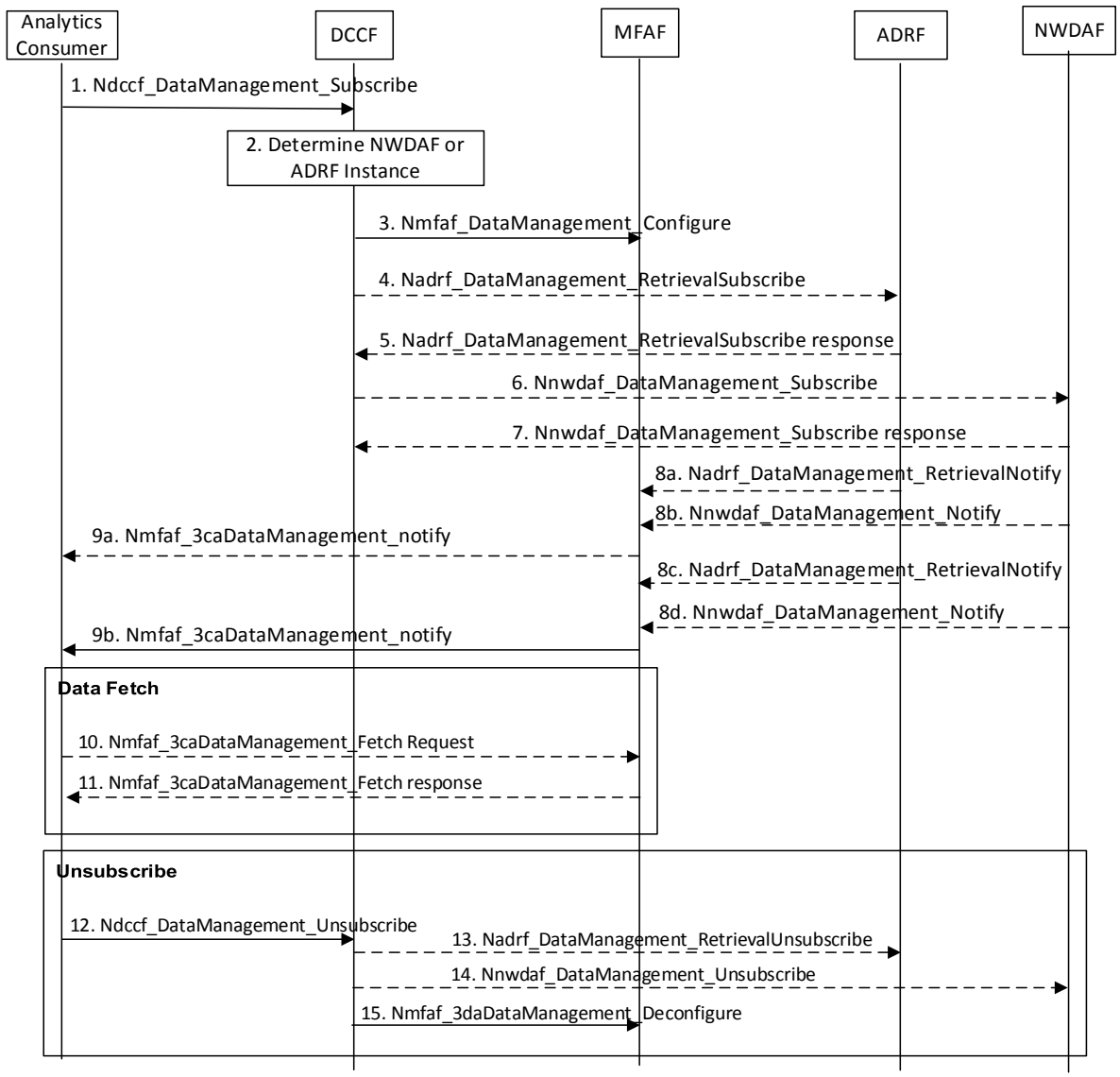

Figure 6.1.4.5-1: Historical Analytics Exposure via Messaging Framework

1. The analytics consumer requests analytics via DCCF by invoking the Ndccf_DataManagement_Subscribe(Nnwdaf service operation, Analytics Specification, Time Window, Formatting Instructions, Processing Instructions, ADRF ID or NWDAF ID (or ADRF Set ID or NWDAF Set ID)). The analytics consumer may specify one or more notification endpoints to receive the analytics.

2. If an ADRF or NWDAF instance or ADRF or NWDAF Set ID is not provided by the Analytics Consumer, the DCCF determines if any ADRF or NWDAF instances might provide the analytics as described in clause 5A and clause 5B.

3. The DCCF sends an Nmfaf_3daDataManagement_Configure(Analytics Consumer Information, Formatting Conditions, Processing Instructions) to configure the MFAF to map notifications received from the ADRF or NWDAF to outgoing notifications sent to endpoints, and to instruct the MFAF how to format and process the outgoing notifications.

   "Analytics Consumer Information" contains for each notification endpoint, the analytics consumer Notification Target Address (+ Analytics Consumer Notification Correlation ID) to be used by the MFAF when sending notifications. The MFAF selects an MFAF Notification Target Address (+ MFAF Notification Correlation ID) and sends the MFAF Notification Information, containing the MFAF Notification Target Address (+ MFAF Notification Correlation ID), to the DCCF in the Nmfaf_3daDataManagement_Configure Response.

4. (conditional) If the DCCF determines that an ADRF instance might provide the analytics, or an ADRF instance or Set was supplied by the Analytics Consumer, the DCCF sends a request to the ADRF, using Nadrf_DataManagement_RetrievalSubscribe(Analytics Specification, MFAF Notification Information) as specified in clause 10.2.6. The MFAF Notification information contains the MFAF Notification Target Address (+ MFAF Notification Correlation ID) received in step 3.

5. The ADRF responds to the DCCF with an Nadrf_DataManagement_RetrievalSubscribe response indicating if the ADRF can supply the analytics. If the analytics can be provided, the procedure continues with step 8.

6. (conditional) If the DCCF determines that an NWDAF instance might provide the analytics or an NWDAF instance or Set was supplied by the Analytics Consumer, the DCCF sends a request to the NWDAF using Nnwdaf_DataManagement_Subscribe (Analytics Specification, MFAF Notification Information) as specified in clause 7.4.2. The MFAF Notification Information contains the MFAF Notification Target Address (+ MFAF Notification Correlation ID) received in step 3.

7. The NWDAF responds to the DCCF with an Nnwdaf_DataManagement_Subscribe response indicating if the NWDAF can supply the analytics.

8. The ADRF uses Nadrf_DataManagement_RetrievalNotify or the NWDAF uses Nnwdaf_DataManagement_Notify to send the requested analytics (e.g. one or more stored notifications archived from an NWDAF) to the MFAF. The analytics may be sent in one or more notification messages.

9. The MFAF uses Nmfaf_3caDataManagement_Notify to send analytics to all notification endpoints indicated in step 3. Notifications are sent to the Notification Target Address(es) using the Analytics Consumer Notification Correlation ID(s) received in step 3. Analytics sent to notification endpoints may be processed and formatted by the DCCF, so they conform to delivery requirements specified by the analytics consumer.

NOTE: According to Formatting Instructions provided by the Analytics Consumer, multiple notifications from an ADRF or NWDAF can be combined in a single Ndccf_DataManagement_Notify so many notifications from the ADRF or NWDAF results in fewer notifications (or one notification) to the Analytics Consumer. Alternatively, a Nmfaf_3caDataManagement_Notify can instruct the analytics notification endpoint to fetch the analytics from the DCCF before an expiry time.

10. If a notification contains a fetch instruction, the notification endpoint sends a Nmfaf_3caDataManagement_Fetch request as specified in clause 9.3.3 to fetch the analytics from the MFAF.

11. The DCCF delivers the analytics to the notification endpoint.

12. When the analytics consumer no longer wants analytics to be collected or has received all the analytics it needs, it invokes Ndccf_DataManagement_Unsubscribe(Subscription Correlation ID) as specified in clause 8.2.3, using the Subscription Correlation Id received in response to its subscription in step 1.

13. If the analytics are being provided by an ADRF and there are no other analytics consumers subscribed to the analytics, the DCCF invokes Nadrf_DataManagement_RetrievalUnSubscribe as specified in clause 10.2.7 to unsubscribe from the ADRF.

14. If the analytics are being provided by an NWDAF and there are no other analytics consumers subscribed to the analytics, the DCCF invokes Nnwdaf_DataManagement_Unsubscribe service operation as specified in clause 7.4.3 to unsubscribe from the NWDAF

15. The DCCF de-configures the MFAF so it no longer maps notifications received from the NWDAF to the notification endpoints configured in step 3.

6.1A Analytics aggregation from multiple NWDAFs

6.1A.1 General

In a multiple NWDAF deployment scenario, an NWDAF instance may be specialized to provide Analytics for one or more Analytics IDs. Each of the NWDAF instances may serve a certain Area of Interest or TAI(s). Multiple NWDAFs may collectively serve the particular Analytics ID. An NWDAF may have the capability to support the aggregation of Analytics (per Analytics ID) received from other NWDAFs, possibly with Analytics generated by itself.

The procedure for analytics aggregation from multiple NWDAFs is as defined in clause 6.1A.3.

6.1A.2 Analytics Aggregation

The analytics aggregation from multiple NWDAFs is used to address cases where an NWDAF service consumer requests Analytics ID(s) that requires multiple NWDAFs to collectively serve the request. Analytic aggregation applies to scenarios where NWDAF service consumer requests or subscribes to analytics information with or without provisioning Area of Interest.

Aggregator NWDAF or aggregation point:

- Is an NWDAF instance with additional capabilities to aggregate output analytics provided by other NWDAFs. This is in addition to regular NWDAF behaviour such as collecting data from other data sources to be able to generate its own output analytics.
- Is able to divide the area of interest, if received from the consumer, into sub area of interest based on the serving area of each NWDAF to be requested for analytics, and then send analytics requests including the sub area of interest as an Analytics Filter to corresponding NWDAFs. The Aggregator NWDAF may maintain information on the discovered NWDAFs, including their supported Analytics IDs, NWDAF Serving Areas, etc.
- Has "analytics aggregation capability" registered in its NF Profile within the NRF.
- Supports the requesting and exchange of "Analytics Metadata Information" between NWDAFs when required for the aggregation of output analytics."Analytics Metadata Information" is additional information associated with the requested Analytics ID(s) as defined in clause 6.1.3.
- Supports dataset statistical properties, output strategy, and data time window parameters per type of analytics (i.e. Analytics ID) as defined in clause 6.1.3.

NRF:

- Stores the NF Profile of the NWDAF instances, including "analytics aggregation capability" for Aggregator NWDAFs and "analytics metadata provisioning capability" when supported by the NWDAF.
    - Returns the NWDAF(s) matching the attributes provided in the Nnrf_NFDiscovery_Request, as specified in clause 5.2.7.3 ofTS 23.502 [3].

NWDAF service consumer:

- Requests or subscribes to receive analytics for one or more Analytics IDs, as specified in clause 6.1 of the present document.
- Uses the discovery mechanism from NRF as defined in clause 6.3.13 ofTS 23.501 [2] to identify NWDAFs with analytics aggregation capability and other capabilities (e.g. providing data/analytics for specific TAI(s)).
- Can differentiate and select the preferred NWDAF in case multiple NWDAFs are returned in the NWDAF discovery response based on its internal selection criteria (considering the registered NWDAF capabilities and information in NRF or UDM).

6.1A.3 Procedure for analytics aggregation

6.1A.3.1 Procedure for analytics aggregation with Provision of Area of Interest

The procedure depicted in figure 6.1A.3-1 is used to address cases where an NWDAF service consumer requests Analytics ID(s) for an Area of Interest that requires multiple NWDAFs that collectively serve the request.

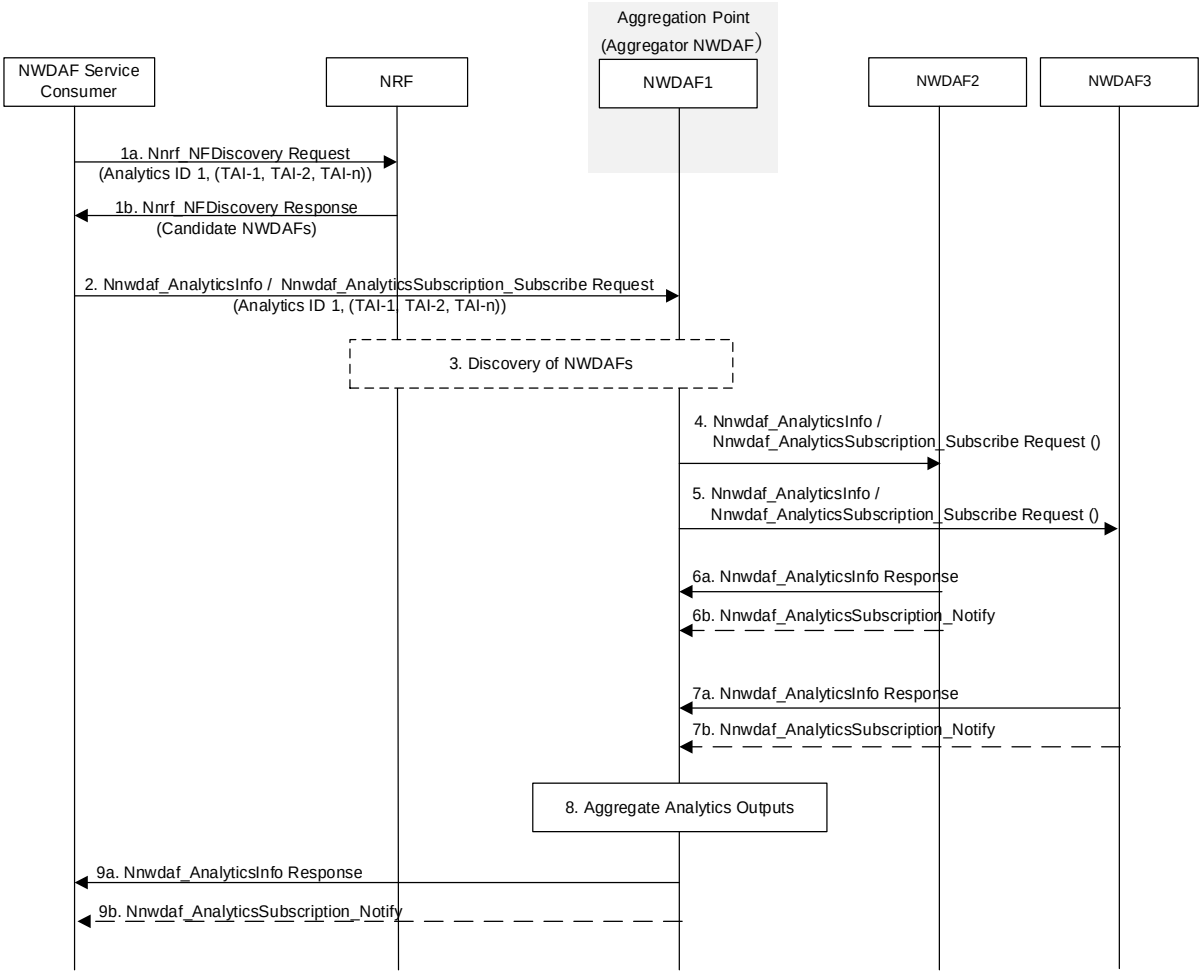

Figure 6.1A.3.1-1: Procedure for analytics aggregation

1a-b. NWDAF service consumer discovers the NWDAF as specified in clause 5.2. When NRF is used, NRF may return multiple NWDAF candidates matching the requested capabilities, area of interest, and supported Analytics ID(s). NWDAF service consumer selects an NWDAF (e.g. NWDAF1) with analytics aggregation capability (i.e. Aggregator NWDAF), based on its internal selection criteria, considering registered NWDAF capabilities and information in NRF including the Supported Analytics Delay per Analytics ID (if available).

2. NWDAF service consumer invokes Nnwdaf_AnalyticsInfo_Request or Nnwdaf_AnalyticsSubscription_Subscribe service operation from the selected Aggregator NWDAF (e.g. NWDAF1). In the request, NWDAF service consumer provides Analytics ID(s) (e.g. Analytics ID 1) Analytics Filter Information (area of interest, e.g. TAI-1, TAI-2, TAI-n, if known to the NWDAF service consumer), Target of Analytics Reporting (e.g. a single UE, a group of UEs or any UE). It may also provide "time when analytics information is needed" (e.g. T1). It is expected that T1 is equal or greater than the Supported Analytics Delay per Analytics ID (if available) of the Aggregator NWDAF. Otherwise, the aggregator NWDAF may reject the analytics request or analytics subscription.

3. On receiving the request in step 2, Aggregator NWDAF (e.g. NWDAF1), based on e.g. configuration, queries to NRF including the Real-Time Communication Indication per Analytics ID and queries to UDM for checking which NWDAF(s) is serving the Target of Analytics Reporting.Considering the request from the NWDAF service consumer (e.g. Analytics Filter Information, T1, etc.) and Supported Delay per Analytics ID per NWDAF instance (when Real-Time Communication Indication was included), Aggregator NWDAF determines the other NWDAF instances that collectively can cover the area of interest indicated in the request (e.g. TAI-1, TAI-2, TAI-n).

NOTE 1: In the discovery request sent to NRF, Aggregator NWDAF might indicate "analytics metadata provisioning capability" (e.g. as query parameter), thus, requesting to NRF to reply back with, if available, those NWDAF instance(s) which also supports "analytics metadata provisioning capability" functionality as indicated during particular NWDAF instance registration procedure.

4-5. Aggregator NWDAF (e.g. NWDAF1) invokes Nnwdaf_AnalyticsInfo_Request or Nnwdaf_AnalyticsSubscription_Subscribe service operation from each of the NWDAFs discovered/determined in step 3 (e.g. NWDAF2 and NWDAF3).

The request may optionally indicate "analyticsmetadata request" parameter to the determined NWDAFs (e.g. NWDAF-2 and/or NWDAF3), when analytics metadata is supported by these NWDAFs.

The request or subscription to the determined NWDAFs (e.g. NWDAF2 and/or NWDAF3) may also include the dataset statistical properties, output strategy, and data time window. This indicates to the determined NWDAFs that the Analytics ID output shall be generated based on such parameters when requested.

If "time when analytics information is needed" (T1) was provided in step 2, the Aggregator NWDAF shall also provide a "time when analytics information is needed" to the determined NWDAFs, with a smaller value compared with T1 (e.g. T2).

NOTE 2: T2 in step 4-5 is smaller than T1 accounting for the analytics delay and processing time within the Aggregator NWDAF itself.

6-7a-b. The determined NWDAFs (e.g. NWDAF-2 and/or NWDAF3) reply or notify with the requested output analytics.

If "analytics metadata request" was included in the request received by such NWDAF (in steps 4-5), the NWDAF additionally returns the "analytics metadata information" used for generating the analytics output as defined in clause 6.1.3.

If the determined NWDAFs (e.g. NWDAF 2 and/or NWDAF 3) cannot reply or notify with the requested output analytics before the expiry of T2, they may send an error response or error notification to the Aggregator NWDAF including a "revised waiting time".

8. Aggregator NWDAF (e.g. NWDAF1) aggregates received Analytics information, i.e. generates a single output analytics based on the multiple analytics outputs and, optionally, the "analytics metadata information" received from the determined NWDAFs (e.g. NWDAF2 and NWDAF3).

The Aggregator NWDAF (e.g. NWDAF1) may also take its own analytics for TAI-n into account for the analytics aggregation.

9a-b. Aggregator NWDAF (e.g. NWDAF1) sends a response or notifies to the NWDAF service consumer the aggregated output analytics for the requested Analytics ID.

If the Aggregator NWDAF (e.g. NWDAF 1) cannot reply or notify with the requested output analytics before the expiry of T1 or anticipates that it cannot reply or notify with the requested output analytics before the expiry of T1 (e.g. due to error notification in step 6-7a-b), it may send an error response or error notification to the NWDAF service consumer including a "revised waiting time". The NWDAF service consumer may optionally use the "revised waiting time" to update the "time when analytics information is needed" parameter (i.e. T1) for future analytics requests/subscriptions to the same Aggregator NWDAF as defined in clause 6.2.5.2.

6.1A.3.2 Procedure for Analytics Aggregation without Provision of Area of Interest

The procedure depicted in Figure 6.1A.3.2-1 is used to address cases where an NWDAF service consumer requests Analytics ID(s) without providing an Area of Interest, but requires multiple NWDAFs to collectively serve the request.

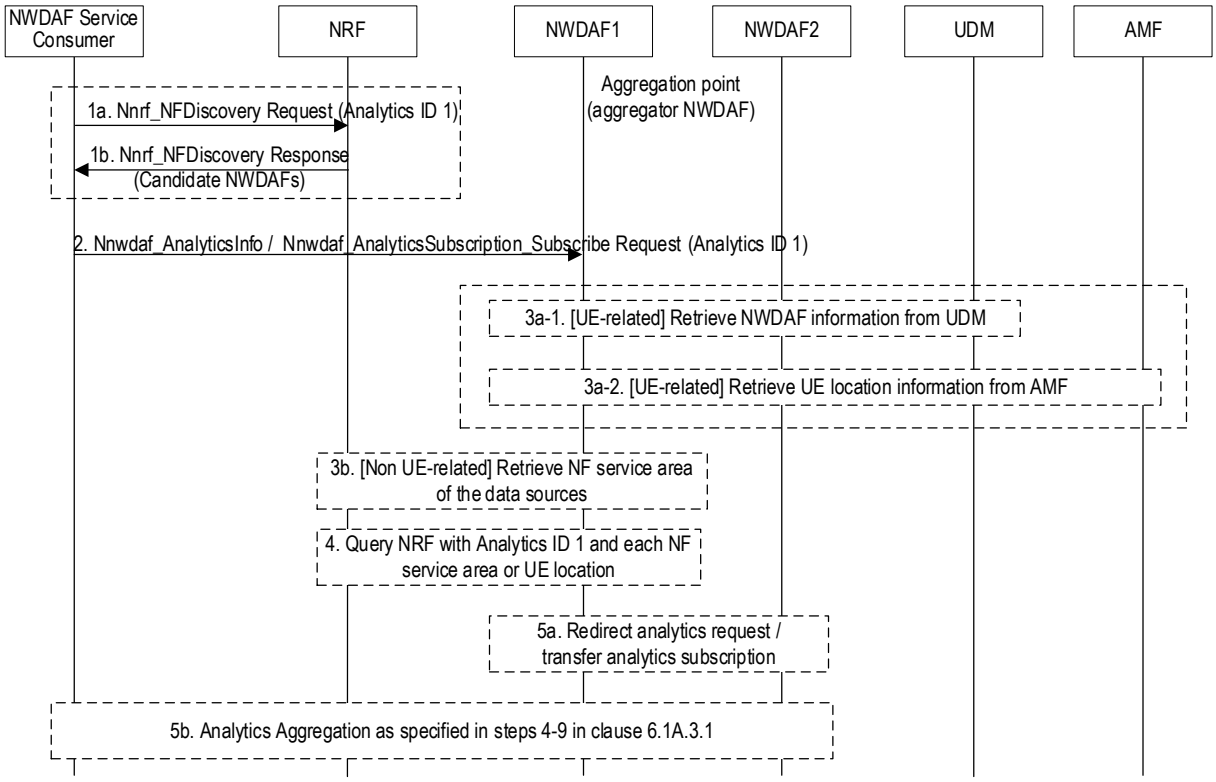

Figure 6.1A.3.2-1: Procedure for analytics aggregation without provision of Area of Interest

1. This step is a NWDAF discovery procedure without providing any area of interest. The service consumer discovers an aggregation NWDAF (e.g. NWDAF1) as specified in clause 5.2. When NRF is used, NRF may return multiple NWDAF candidates matching the requested capabilities and supported Analytics ID(s).

   Depending on the requested Analytics ID, the NWDAF service consumer, e.g. based on internal logic, can be able to determine which NWDAF should be selected for providing the required data analytics. If not, the NWDAF service consumer should select a NWDAF with large serving area from the candidate NWDAFs which supports analytics aggregation, e.g. NWDAF1.

2. NWDAF service consumer sends Analytics information or analytics subscription request to the aggregator NWDAF, i.e. NWDAF1 in the Figure 6.1A.3.2-1. In the request, NWDAF service consumer provides the requested Analytics ID(s), e.g. Analytics ID 1.

   The NWDAF service consumer may also provide "time when analytics information is needed" (e.g. T1). It is expected that T1 is equal or greater than the Supported Analytics Delay per Analytics ID of the Aggregator NWDAF (if available). Otherwise, the aggregator NWDAF may reject the analytics request or analytics subscription.

   Once receiving the request, the Aggregator NWDAF1 may decide to subscribe data analytics from other NWDAF instances which can provide the requested data analytics. Based on the Analytics ID, there are two cases for the Aggregator NWDAF1 to subscribe data analytics from other NWDAF instances.

3a. If the data analytics requires UE location information, e.g. for the Analytics IDs "UE Mobility", "Abnormal behaviour", or "User Data Congestion", then:

   - 3a-1: (optional) The Aggregator NWDAF1 queries UDM to discover the NWDAF serving the UE, if it is supported.

   - 3a-2: If step 3a-1 is not supported, was not executed, or did not return a suitable NWDAF serving the UE, the Aggregator NWDAF1 determines the AMF serving the UE as specified in the clause 6.2.2.1, then requests UE location information from the AMF to be used in the query to NRF in step 4.

NOTE: If an Aggregator NWDAF receives an Analytics request for a group of UEs, i.e. the Target of Analytics Reporting set to an Internal Group ID, it performs NWDAF discovery based on location information of all UEs in the group, and then requests all discovered NWDAFs to provide the required analytics.

3b. If the data analytics does not require to collect UE location information, e.g. for the Analytics IDs "Service Experience", "NF load information", or "UE Communication", the Aggregator NWDAF1 can determine the NFs to be contacted for data collection as specified in clause 6.2.2.1 and then it can retrieve NF service area for each of the data source NF from NRF.

4. (conditional) With the data obtained in step 3, the Aggregator NWDAF1 queries the NRF for discovering the required NWDAF, by sending an NF discovery request including UE location (e.g. TAI-1) or NF serving area (e.g. TAI list-1) as a filter to NRF, and obtains candidates target NWDAF(s) that can provide the required analytics. This step is skipped if a suitable NWDAF was discovered in step 3a-1. Additionally the Aggregator NWDAF1 may include in the NF discovery request the Real-Time Communication Indication per Analytics ID to request Supported Delay per Analytics ID per NWDAF instance.

   Depending on the discovered NWDAF instance(s), there can be two cases:

   5a. If a single target NWDAF (e.g. NWDAF2) can provide the requested analytics data, the Aggregator NWDAF (e.g. NWDAF1) can redirect the Nnwdaf_AnalyticsInfo_Request to that target NWDAF or request an analytics subscription transfer to that target NWDAF, depending on the type of the analytics request/subscription received by the NWDAF Service Consumer.

   5b. If the Aggregator NWDAF decides to request data analytics from one or more target NWDAFs, the steps 4-9 of the analytics aggregation procedure in clause 6.1A.3.1 are executed.

6.1B Transfer of analytics context and analytics subscription

6.1B.1 General

In a multiple NWDAFs deployment scenario, procedures for transfer of analytics context and analytics subscription can be used to support the target NWDAF to produce the needed analytics.

When the analytics consumer provides the target NWDAF with information on the subscription that could be transferred from the source NWDAF, the target NWDAF may initiate the transfer of analytics context. The analytics consumer provides the information via Nnwdaf_AnalyticsSubscription_Subscribe service operation. When the analytics consumer is an AMF, the old subscription information (if related to a UE) may be provided by the source AMF to the target AMF using a UE context transfer procedure as specified in TS 23.502 [3].

An analytics subscription transfer to the target NWDAF may be initiated by the source NWDAF, followed by an analytics context transfer initiated by the target NWDAF. An NWDAF may transfer one or more of its analytics subscriptions to another NWDAF instance due to internal (e.g. load balancing, graceful shutdown) or external triggers (e.g. UE mobility). For external triggers, the NWDAF may subscribe to NF(s) to be notified about the corresponding events. As for UE mobility, upon the UE location change event notified by the AMF subscribed by the NWDAF, the NWDAF determines whether it can continue to provide the analytics service. If the NWDAF cannot continue to serve the consumer, it should either select a target NWDAF and initiate analytics subscription transfer, or notify the analytics consumer that it cannot provide the service anymore, so that the analytics consumer can select a new NWDAF.

Procedures for analytics subscription transfer allow one NWDAF instance to transfer its ongoing analytics subscriptions to another NWDAF instance. The transfer can be done for all subscriptions or just a selected subset of subscriptions related to specific area(s), specific Analytics ID(s), specific NF(s) and/or specific UE(s).

The procedure for prepared analytics subscription transfer can be used if the source NWDAF instance anticipates that it will soon not be able to continue its current analytics tasks.

6.1B.2 Analytics Transfer Procedures

6.1B.2.1 Analytics context transfer initiated by target NWDAF selected by the NWDAF service consumer

The procedure in Figure 6.1B.2.1-1 is used when an NF decides to select a new NWDAF instance due to internal or external triggers, e.g. the NF starts serving a UE with analytics subscription information received upon UE context transfer procedure as described in TS 23.502 [3], or the NF starts to request NF related analytics, or the NF receives a "Termination Request" for an existing analytics subscription from an NWDAF. The NF sends to the target NWDAF information about the NWDAF previously used for analytics subscription, if available, in Nnwdaf_AnalyticsSubscription_Subscribe service operation. The target NWDAF may initiate the transfer of the analytics context, using the Nnwdaf_AnalyticsInfo_ContextTransfer or Nnf_DataManagement_Subscribe service operation.

The procedure in Figure 6.1B.2.1-1 is also used when an Aggregator NWDAF decides to select a new NWDAF to request output analytics for analytics aggregation. For example, upon receiving a Termination Request from one of the NWDAFs that are collectively serving a request for analytics subscription as specified in clause 6.1A, the Aggregator NWDAF queries the NRF or UDM to select a target NWDAF as specified in clause 6.1A.3 using information e.g. the UE location, the 5GC NFs (identified by their NF Set IDs or NF types) serving the UE or to be contacted for data collection (if Area of Interest is not provisioned for the requested analytics), or the subset of AoI (if Area of Interest is provisioned for the requested analytics). Then, the Aggregator NWDAF sends information about the NWDAF previously used for analytics subscription, if available, in Nnwdaf_AnalyticsSubscription_Subscribe service operation towards the selected target NWDAF.

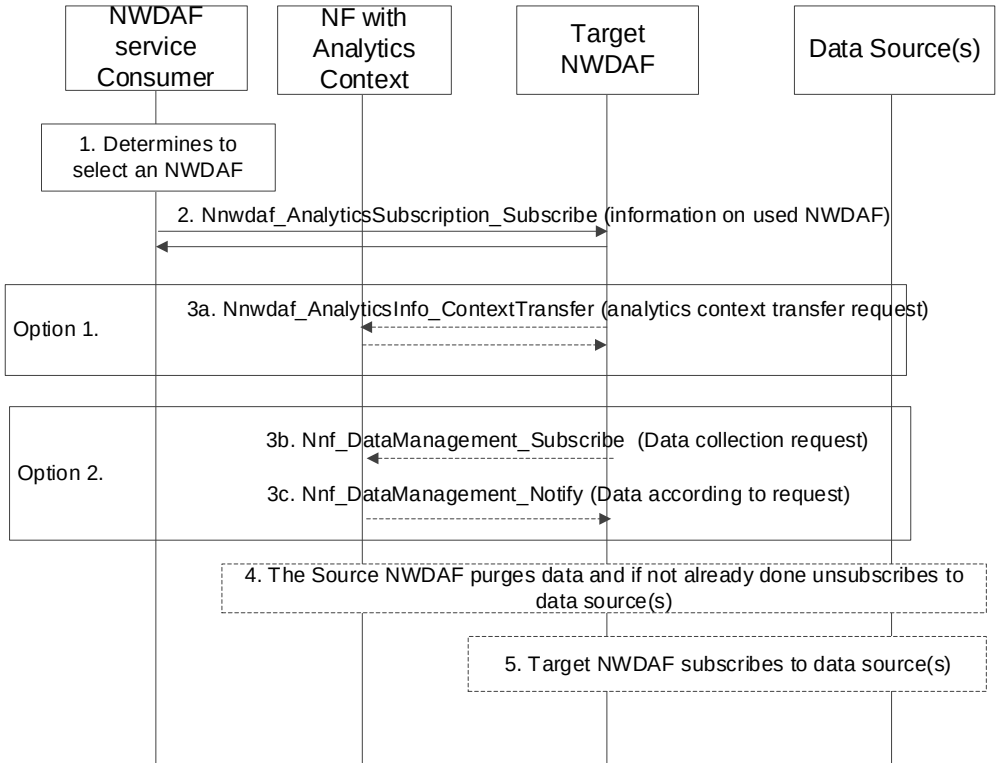

Figure 6.1B.2.1-1: Analytics context transfer initiated by target NWDAF selected by the NWDAF service consumer

1. The NWDAF service consumer determines to select an NWDAF instance. The consumer discovers and selects the target NWDAF as specified in clause 5.2.

2. The consumer sends a request for analytics subscription to the target NWDAF using Nnwdaf_AnalyticsSubscription_Subscribe service operation, including information on the previous analytics subscription (e.g., NWDAF ID and Subscription Correlation ID) which relates to the requested analytics

subscription, if available. If the target NWDAF accepts the analytics subscription request, it sends Nnwdaf_AnalyticsSubscription_Subscribe response with a Subscription Correlation ID.

If the target NWDAF does not receive information of previous analytics subscription in step 2, for UE related Analytics, the target NWDAF may discover previously used NWDAF in UDM as specified in clause 5.2.

NOTE: If the selected target NWDAF instance is the same as the source NWDAF instance (as received from the other consumer in step 0), the target NWDAF will update the existing analytics subscription to the new analytics consumer. Following steps are skipped.

3a. [Option 1] If the target NWDAF decides to request an analytics context transfer from the previously used NWDAF, it may make use of information sent in step 2 (e.g., the provided Subscription Correlation ID) and use the analytics context transfer procedure as specified in clause 6.1B.3. The target NWDAF may receive an ADRF ID or DCCF ID for collecting the historical data and/or analytics.

3b-c. [Option 2] If the target NWDAF decides to only request historical data and/or analytics, then it may collect the data and/or analytics via Nnf_DataManagement_Subscribe service, where the NFs may be either the ADRF, NWDAF or DCCF, as described in clauses 10.2.6, 7.4.2 and 8.2.2 respectively.

Target NWDAF is now ready to generate analytics information taking into account the information received in step 3.

4. [Optional] Source NWDAF may purge analytics context after completion of step 3a, if performed, and if not already done, unsubscribes from the data source(s) and/or model source(s) that are no longer needed for the remaining analytics subscriptions.

5. [Optional] Target NWDAF may subscribe to relevant data source(s) and/or model source(s), if it is not yet subscribed to the data source(s) and/or model source(s).

6.1B.2.2 Analytics Subscription Transfer initiated by source NWDAF

The procedure in Figure 6.1B.2.2-1 is used by an NWDAF instance to request the transfer of analytics subscription(s) to another NWDAF instance, using the Nnwdaf_AnalyticsSubscription_Transfer service operation defined in clause 7.2.5.

If the source NWDAF discovers that the analytics consumer may change concurrently to this procedure, the source NWDAF should not perform the procedure. In such a case, the source NWDAF may send a message to indicate to the analytics consumer that it will not serve this subscription anymore.

NOTE 1: To discover the possible change of analytics consumer, if the Analytics ID is UE related, the source NWDAF takes actions responding to external trigger (such as UE mobility), for example, checking if the Target of Analytics Reporting is still within the serving area of the analytics consumer, if the serving area information is available.

NOTE 2: Handling of overload situation or preparation for a graceful shutdown are preferably executed inside an NWDAF Set, when available, therefore, not requiring an analytics subscription transfer as described in this clause. The procedure in Figure 6.1B.2.2-1 is applicable for analytics subscription transfer across NF Sets or if the NWDAF is not deployed in a Set.

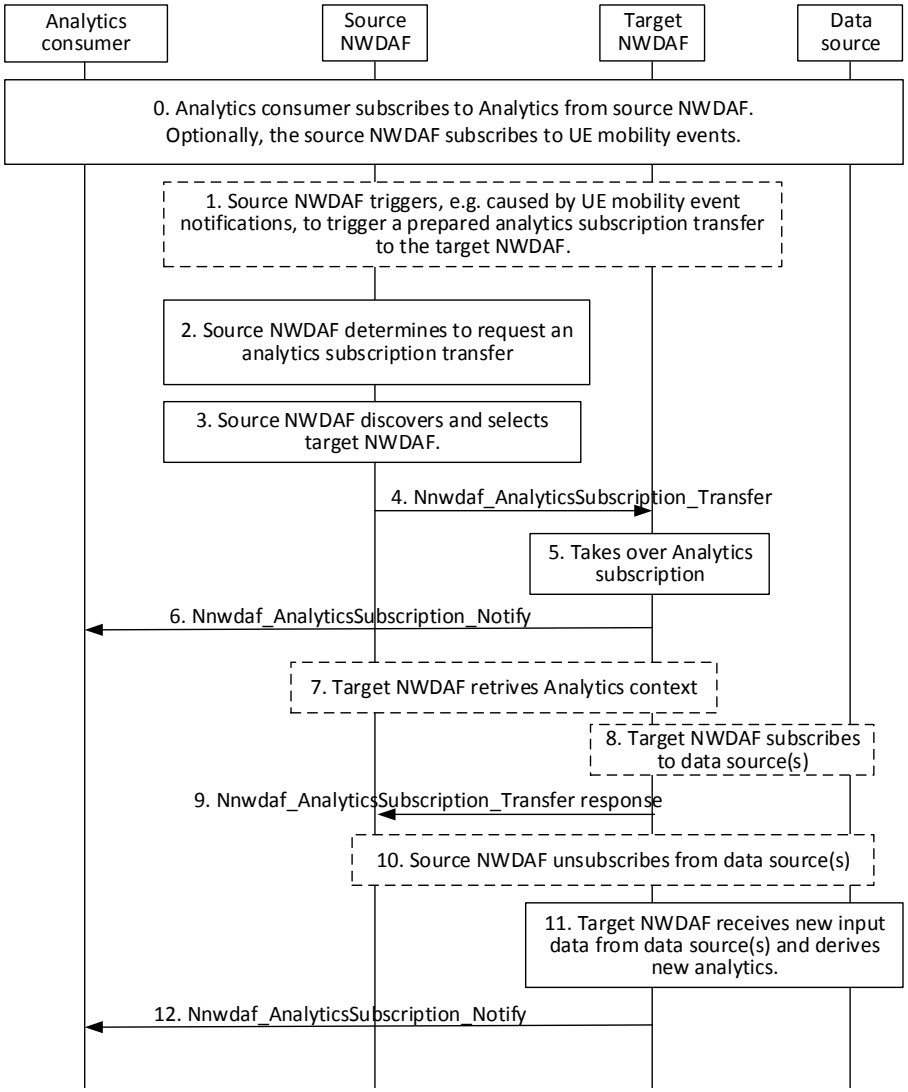

Figure 6.1B.2.2-1: Analytics subscription transfer initiated by source NWDAF

0. The analytics consumer subscribes to analytics from source NWDAF. The analytics consumer may send its NF ID or serving area, enabling NWDAF to determine whether the following analytics subscription transfer procedure is applicable. Optionally the source NWDAF subscribes to UE mobility events.

1. [Optional] Source NWDAF determines, e.g. triggered by a UE mobility event notification, to prepare an analytics subscription transfer to target NWDAF(s), as specified in the procedure illustrated in clause 6.1B.2.3.

2. Source NWDAF determines, e.g. based on the UE location information received and the analytics consumer's serving area either directly received in step 0 or indirectly received via NRF, to perform an analytics subscription transfer to target NWDAF(s). Therefore, the source NWDAF determines the analytics subscription(s) to be transferred to a target NWDAF.

3. Source NWDAF performs an NWDAF discovery and selects the target NWDAF. NWDAF discovery may be skipped if the target NWDAF had already been discovered as part of a prepared analytics subscription transfer. In the case of aggregated analytics from multiple NWDAFs, the source NWDAF may use the set of NWDAF identifiers related to aggregated analytics (see clause 6.1.3) to preferably select a target NWDAF that is already serving the consumer.

4. Source NWDAF requests, using Nnwdaf_AnalyticsSubscription_Transfer Request service operation, a transfer of the analytics subscription(s) determined in step 2 to the target NWDAF. The request contains a callback URI of the analytics consumer. The request also contains active data source ID(s), ML model information and/or ID(s) of NWDAF(s) containing MTLF, which are related to the analytics subscriptions requested to be transferred, if not already provided as part of the prepared analytics subscription transfer in the preparation

procedure (see step 1). The request message may also include "analytics context identifier(s)" indicating the availability of analytics context for particular Analytics ID(s).

5. Target NWDAF accepts the analytics subscription transfer and takes over the analytics generation based on the information received from the source NWDAF.

   Target NWDAF may use the ML model information, if provided in the Nnwdaf_AnalyticsSubscription_Transfer request, to retrieve the ML model(s) and use it for the transferred analytics subscription. If the ID(s) of NWDAF(s) containing MTLF is provided in the Nnwdaf_AnalyticsSubscription_Transfer request, target NWDAF may request or subscribe to the ML model(s) from the indicated NWDAF(s) containing MTLF as specified in clause 6.2A, taking account of the locally configured set of NWDAFs containing MTLF if any, and use the ML model(s) for the transferred analytics subscription.

NOTE 3: If not yet done during a prepared analytics subscription transfer, the target NWDAF allocates a new Subscription Correlation ID to the received analytics subscriptions.

NOTE 4: The target NWDAF might already have received information on some/all of the analytics subscriptions as part of the prepared analytics subscription transfer request received in step 1 and, thus, might already have started to prepare for the analytics generation, e.g. by having already subscribed to relevant event notifications.

6. Target NWDAF informs the analytics consumer about the successful analytics subscription transfer using a Nnwdaf_AnalyticsSubscription_Notify message. A new Subscription Correlation ID, which was assigned by the target NWDAF, is provided in the Subscription Correlation ID and the old Subscription Correlation Id, which was allocated by the source NWDAF, is provided in the Subscription Change Notification Correlation ID parameter of this message as specified in clause 7.2.4.

NOTE 5: Notification correlation information in the Nnwdaf_AnalyticsSubscription_Notify message allows the analytics consumer to correlate the notifications to the initial subscription request made with the source NWDAF in step 0.

NOTE 6: The existing Analytics context in the source NWDAF is not deleted directly but will be purged first when it was collected by the target NWDAF.

NOTE 7: If this subscription is used as input for analytics aggregation by the analytics consumer, the analytics consumer might inform the other NWDAFs instance participating in this analytics aggregation that the Set of NWDAF identifiers of NWDAF instances used by the NWDAF service consumer for this analytics aggregation (see clause 6.1.3) has changed using the Nnwdaf_AnalyticsSubscription_Subscribe service operation.

7. [Conditional] If "analytics context identifier(s)" had been included in the Nnwdaf_AnalyticsSubscription_Transfer Request received in step 4, the target NWDAF requests the "analytics context". The analytics context transfer procedure is specified in clause 6.1B.3.

8. [Optional] Target NWDAF subscribes to relevant data source(s), if it is not yet subscribed to the data source(s) for the data required for the Analytics.

9. Target NWDAF confirms the analytics subscription transfer to the source NWDAF.

10. [Optional] Source NWDAF unsubscribes with the data source(s) that are no longer needed for the remaining analytics subscriptions. In addition, Source NWDAF unsubscribes with the NWDAF(s) containing MTLF, if exist, which are no longer needed for the remaining analytics subscriptions.

NOTE 8: At this point, the analytics subscription transfer is deemed completed, i.e. the source NWDAF can delete all information related to the successfully transferred analytics subscription.

11-12. Target NWDAF at some point derives new output analytics based on new input data and notifies the analytics consumer about the new analytics using a Nnwdaf_AnalyticsSubscription_Notify message as specified in clause 6.1.1.

6.1B.2.3 Prepared analytics subscription transfer

The procedure in Figure 6.1B.2.3-1 is used by an NWDAF instance to request another NWDAF instance for a prepared analytics subscription transfer from the source NWDAF instance, using the Nnwdaf_AnalyticsSubscription_Transfer service operation defined in clause 7.2.5.

NOTE 1: The source NWDAF might determine that it needs to prepare to transfer analytics to another NWDAF instance, e.g. when the source NWDAF estimates for UE related analytics subscription that the UE might enter an area which is not covered by the source NWDAF (e.g., by subscribing to AMF event exposure service for UE mobility event notifications, by performing UE mobility analytics, or by subscribing to another NWDAF providing UE mobility analytics). If the source NWDAF discovers that the analytics consumer may change concurrently to this procedure, the source NWDAF does not perform the procedure. If the procedure makes use of predictions to determine the candidate NWDAFs, care must be taken with regards to load and signalling cost when sending data to an NWDAF that will not eventually start serving the UE.

NOTE 2: The source NWDAF might also determine that it needs to prepare to transfer analytics subscriptions to another NWDAF instance, as the source NWDAF wants to resolve an internal load situation or prepare for a graceful shutdown.

NOTE 3: Handling of overload situation or preparation for a graceful shutdown are preferably executed inside an NWDAF Set, when available.

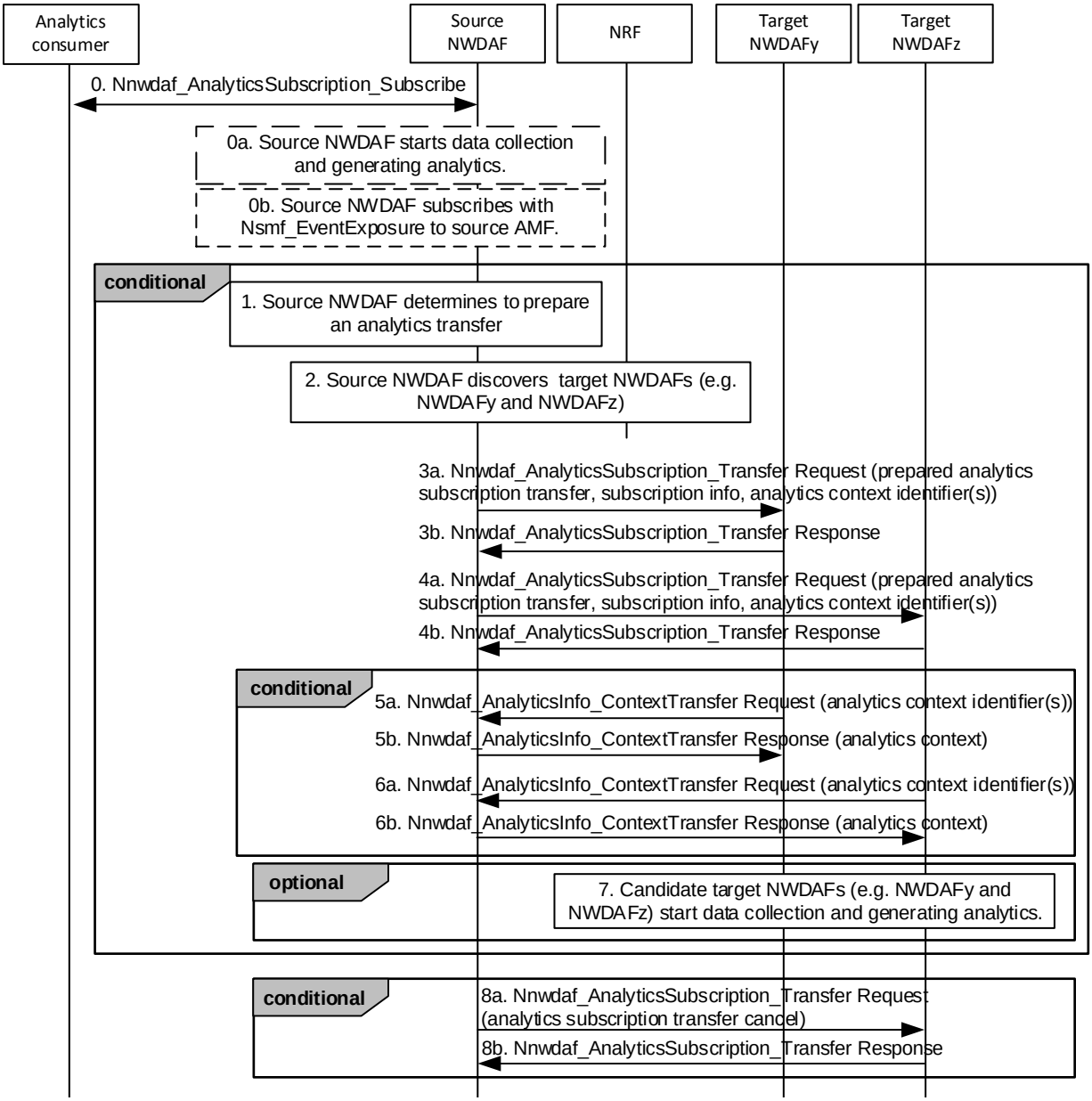

Figure 6.1B.2.3-1: Prepared analytics transfer

0. Analytics consumer subscribes to the source NWDAF for certain analytics as specified in clause 6.1.1.

0a. Source NWDAF starts data collection from relevant data source(s) (e.g. NFs or OAM) as specified in clause 6.2. Source NWDAF starts generating requested analytics.

0b. [Conditional] (Only if the source NWDAF does not serve the whole PLMN and the requested analytics involves UE related data) The source NWDAF subscribes, using Namf_EventExposure_Subscribe service operation, to receive notifications on UE mobility events from AMF.

1. The source NWDAF determines that it needs to prepare to transfer analytics to another NWDAF instance.

2. The source NWDAF discovers candidate target NWDAF instances (e.g. NWDAFy and NWDAFz) supporting the requested analytics information for the predicted target area(s). NWDAF discovery and selection is specified in clause 6.3.13 ofTS 23.501 [2]. In the case of aggregated analytics from multiple NWDAFs, the source NWDAF may use the set of NWDAF identifiers related to aggregated analytics (see clause 6.1.3) to preferably select a target NWDAF that is already serving the consumer.

NOTE 4: In this procedure, NWDAFy and NWDAFz are examples for target NWDAF instances that are candidates to take over those analytic subscriptions.

3-4. In the case of a prepared analytics subscription transfer, the source NWDAF requests, using Nnwdaf_AnalyticsSubscription_Transfer Request, to the candidate target NWDAFs (e.g. NWDAFy and NWDAFz) to prepare for an analytics subscription transfer by including a "prepared analytics subscription transfer indication" in the request message. The request message includes information on the analytics subscriptions to be transferred. The request message may also include "analytics context identifier(s)" indicating the availability of analytics context for particular Analytics ID(s).

The candidate target NWDAFs (e.g. NWDAFy and NWDAFz) respond to the request from the source NWDAF using a Nnwdaf_AnalyticsSubscription_Transfer Response message.

5-6. [Conditional] If "analytics context identifier(s)" had been included in the Nnwdaf_AnalyticsSubscription_Transfer Request received in step 4, the determined target NWDAFs (e.g. NWDAFy and NWDAFz) may request the "analytics context" from the source NWDAF by invoking the "Nnwdaf_AnalyticsInfo_ContextTransferservice" operation. The analytics context transfer procedure is specified in clause 6.1B.3.

NOTE 5: The target NWDAFs (e.g. NWDAFy and NWDAFz)can allocate a new Subscription Correlation ID to the received analytics subscriptions.

7. [Optional] Based on the information received from the source NWDAF, the target NWDAFs (e.g. NWDAFy and NWDAFz) start data collection from NFs or OAM (as specified in clause 6.2) and analytics generation for the indicated analytics subscriptions.

NOTE 6: After step 7, the source NWDAF initiates the analytics subscription transfer to the target NWDAF as specified in steps 4 to 12 of the analytics subscription transfer procedure illustrated in Figure 6.1B.2.2-1.

8. The source NWDAF cancels the prepared analytics subscription transfer to a candidate target NWDAF (e.g. NWDAFz), using Nnwdaf_AnalyticsSubscription_Transfer Request include an "analytics subscription transfer cancel indication". The target NWDAF (e.g. NWDAFz) confirms the cancelation to the source NWDAF and, if applicable, deletes any analytics data that is no longer needed. If the target NWDAF (e.g. NWDAFz), as part of the analytics subscription preparation, had already subscribed to entities to collect data or acquire ML model, it unsubscribes to those entities if the subscriptions are not needed for other active analytics subscriptions with the target NWDAF.

   Step 8 may take place any time after step 4 if the NWDAF determines that the candidate target NWDAF (e.g. NWDAFz) does no longer need to prepare for the analytics subscription transfer. In particular, the source NWDAF shall cancel the prepared analytics subscription transfer to all remaining candidate target NWDAFs after one target NWDAF has accepted the analytics subscription transfer (see NOTE 6).

6.1B.3 Analytics Context Transfer

The procedure depicted in Figure 6.1B.3-1 is used by an NWDAF instance to request analytics context from another NWDAF instance, using the Nnwdaf_AnalyticsInfo_ContextTransfer service operation as defined in clause 7.3.3. This procedure, for example, can be invoked in the procedures described in clause 6.1B.2 to request the transfer of relevant analytics context.

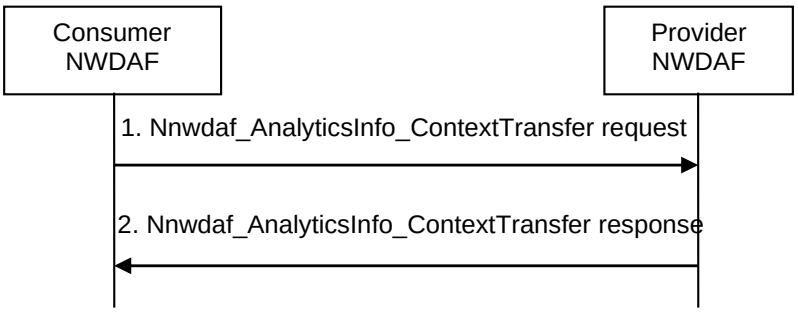

Figure 6.1B.3-1: Analytics Context Transfer

The procedure of analytics context information transfer comprises the following steps:

1. The consumer NWDAF requests analytics context by invoking Nnwdaf_AnalyticsInfo_ContextTransfer request service operation. The parameters that can be provided in the request are listed in clause 6.1B.4.

2. The provider NWDAF responds with analytics context to the consumer NWDAF. The analytics context that can be provided in the response is listed in clause 6.1B.4.

   If the provider NWDAF stores analytics context (i.e. Historical output Analytics and/or Data related to Analytics) in ADRF, the provider NWDAF may include in the response the ADRF ID together with an indication of the Analytics Context Type stored in the ADRF (i.e. Historical output Analytics and/or Data related to Analytics).

   Upon receiving the analytics context, the consumer NWDAF may:

   - provide the pending output analytics or historical analytics information to the analytics consumer per the subscription/request;
   - use the historical data and analytics metadata in the analytics context to generate analytics;
   - subscribe to data collected for analytics with the data sources indicated in the analytics context;
   - retrieve the ML model(s) indicated in the analytics context and use for analytics;
   - subscribe to trained ML model(s) from the indicated NWDAF(s) containing MTLF and use for analytics; and/or
   - subscribe to output analytics from the indicated NWDAFs that collectively serve the transferred analytics subscription and perform analytics aggregation on the output analytics using the analytics metadata information, based on the analytics subscription aggregation information.

6.1B.4 Contents of Analytics Context

The Nnwdaf_AnalyticsInfo_ContextTransfer service operation is used to transfer analytics context from a source NWDAF instance to a target NWDAF instance, whereby the target NWDAF consumes the Nnwdaf_AnalyticsInfo_ContextTransfer service operation produced by the source NWDAF instance to request the analytics context as depicted in Figure 6.1B.3-1.

The consumers of the Nnwdaf_AnalyticsInfo_ContextTransfer service operation (as specified in clause 7.3.3) provide the following input parameters:

- A list of analytics context identifier(s): identify a set of analytics context that are available at the NWDAF instance providing this service and that are requested to be transferred to the consumer NWDAF instance. The analytics context identifier is provided as the following:
  - Subscription Correlation ID: identifies the analytics subscription for which the related analytics context is requested; or
  - A set of SUPI and associated Analytics ID for UE related Analytics; or
  - An Analytics ID for NF related Analytics.
- [OPTIONAL] Requested Analytics Context Type per analytics context identifier: indicates which part of the analytics context the consumer wishes to receive. Following values are specified:
  - Pending output Analytics;
  - Historical output Analytics;
  - Analytics subscription aggregation information;
  - Data related to Analytics;
  - Aggregation related information;
  - Model related information.

NOTE: A list of "analytics context identifier(s)" can be provided by the source NWDAF to the target NWDAF in an analytics subscriptions transfer request as described in clause 6.1B.2.2.Information allowing to identify an analytics context can also be provided by the NWDAF consumer to the target NWDAF in the Nnwdaf_AnalyticsSubscription_Subscribe request and based on this information the target NWDAF derives the "analytics context identifier", as defined in clause 6.1B.2.1.

The producer NWDAF provides to the consumer of the Nnwdaf_AnalyticsInfo_ContextTransfer service operation (as specified in clause 7.3.3), the output information listed below:

- (Set of) Analytics context matching the input parameters of the Nnwdaf_AnalyticsInfo_ContextTransfer request. If no Requested Analytics Context type parameters are available in the request, all available analytics context types are sent. Analytics context includes the following information parts, if available:
  - Analytics related:
    - Pending output analytics (i.e. not yet notified to the consumer).
    - Historical output analytics information. The content of the output analytics is specified in clause 6.1.3 as output information of the Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request service operations.
    - Timestamp(s) of the last output analytics provided to the analytics consumer(s). Value is set to 0 if no output analytics had been sent yet.
    - Analytics subscription aggregation information (only provided when analytics context is related to analytics aggregation): information about the analytics subscriptions that the source NWDAF has with the NWDAFs that collectively serve the transferred analytics subscription, which includes IDs and analytics metadata information of these NWDAFs for specific Analytics ID(s), and optionally input parameters of analytics exposure as defined in clause 6.1.3.
  - Data related to Analytics:
    - Historical data that is available at the source NWDAF and that is related to the analytics to be handed over to the target NWDAF. If available, the time period of the collected data, NF ID(s) of the data source(s) and information (e.g. filter and event reporting parameters) on the subscriptions with those data sources which were used to generate this historical data.
  - Aggregation related information: Related to analytic consumers that aggregate analytics from multiple NWDAF subscriptions:
    - (Set of) NWDAF identifiers of NWDAF instances used by the NWDAF service consumer when aggregating multiple analytic subscriptions.
  - ML Model related information:
    - ID(s) of NWDAF(s) containing MTLF: Instance/Set ID(s) of the NWDAF(s) containing MTLF from which the source NWDAF currently subscribes to the ML Model Information used for the analytics.

6.1C NWDAF Registration/Deregistration in UDM

6.1C.1 General

The procedures in this clause are applicable to UE-related analytics (e.g., UE mobility analytics) for some network deployments, e.g. such with an NWDAF co-located to an AMF or SMF, where the NWDAF is configured to register in UDM for the UEs that it is serving or collecting data for, and for the related Analytics ID(s). This enables NWDAF service consumers to discover the NWDAF instance that is already serving the UE for one or more Analytics ID(s).

6.1C.2 NWDAF Registration in UDM

Figure 6.1C.2-1 shows the procedures for registration of the NWDAF in UDM for UE-related analytics.

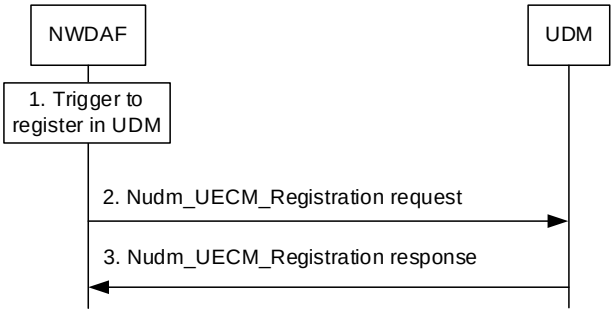

Figure 6.1C.2-1: NWDAF registration in UDM

1. NWDAF triggers a registration in UDM, e.g. based on local configuration in the NWDAF, the reception of a new Analytics subscription request, start of collection of UE related data or an OAM configuration action.
2. The NWDAF registers into UDM for the served UE, by sending Nudm_UECM_Registration request (UE ID, NWDAF ID, Analytics ID(s)).
3. UDM sends a response to NWDAF.

6.1C.3 NWDAF De-registration from UDM

Figure 6.1C.3-1 shows the procedures for deregistration of the NWDAF in UDM.

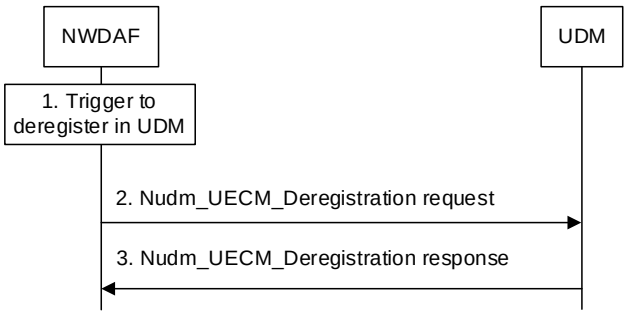

Figure 6.1C.3-1: NWDAF de-registration from UDM

1. NWDAF triggers a de-registration from a previous registration in UDM. This trigger may be that, e.g. the NWDAF has purged the analytics context for the UE (see clause 6.1B.4) for related Analytics ID(s), the NWDAF is no longer collecting data related to the UE, or an administrative action.
2. NWDAF sends Nudm_UECM_Deregistration request (UE ID, NWDAF ID, Analytics ID(s)).
3. UDM sends a response to NWDAF.

6.2 Procedures for Data Collection

6.2.1 General

The Data Collection feature permits NWDAF to retrieve data from various sources (e.g. NF such as AMF, SMF, PCF, and AF; OAM), as a basis of the computation of network analytics.

All available data encompass:

- OAM global NF data,
- Data available in NFs, e.g. behaviour data related to individual UEs or UE groups (e.g. UE reachability), and pre-computed metrics covering UE populations (e.g. number of UEs present in a geographical area), per spatial and temporal dimensions (e.g. per region for a period of time),
- NF data available in the 5GC (e.g. NRF),
- Data available in AF.

When DCCF, ADRF, MFAF or NWDAF hosting DCCF or ADRF are present in the network, the data collection also follows the principles described in clause 6.2.6.

The NWDAF shall use at least one of the following services:

- the Generic management services as defined in TS 28.532 [6], the Performance Management services as defined in TS 28.550 [7] or the Fault Supervision services as defined in TS 28.545 [9], offered by OAM in order to collect OAM global NF data.
- the Exposure services offered by NFs in order to retrieve data and other non-OAM pre-computed metrics available in the NFs.
- Other NF services in order to collect NF data (e.g. NRF)
- DCCF data management service to retrieve data using DCCF.

The NWDAF shall obtain the proper information to perform data collection for a UE, a group of UEs or any UE:

- For an Analytics ID, NWDAF is configured with the corresponding NF Type(s) and/or event ID(s) and/or OAM measurement types.
- NWDAF shall determine which NF instance(s) of the relevant NF type(s) are serving the UE, the group of UEs or any UE, taking into account the S-NSSAI(s) and area of interest as defined in clause 7.1.3 ofTS 23.501 [2].
- NWDAF invokes Nnf_EventExposure_Subscribe services to collect data from the determined NF instance(s), and/or triggers the procedure in clause 6.2.3.2 to subscribe to OAM services to collect the OAM measurement.

The NWDAF performs data collection from an AF directly as defined in clause 6.2.2.2 or via NEF as defined in clause 6.2.2.3. According to the data collection request, the AF may further perform data collection from UE (see clause 6.4.2 and clauses 6.5.2-6.5.4) as defined in clause 6.2.8.

The NWDAF shall be able to discover the events supported by a NF.

Data collection procedures enables the NWDAF to efficiently obtain the appropriate data with the appropriate granularity.

When a request or subscription for statistics or predictions is received, the NWDAF may not possess the necessary data to perform the service, including:

- Data on the monitoring period in the past, which is necessary for the provision of statistics and predictions matching the Analytics target period.
- Data on longer monitoring periods in the past, which is necessary for model training.

Therefore, in order to optimize the service quality, the NWDAF may undertake the following actions:

- The NWDAF may return a confidence parameter as stated in clause 6.1.3 expressing the confidence in the prediction produced. Prediction may be returned with zero confidence as described below. This confidence is likely to grow in the case of subscriptions.
- The value of the confidence depends on the level or urgency expressed by the parameter "preferred level of accuracy" as listed in clause 6.1.3, the parameter "time when analytics information is needed" as listed in clause 6.1.3, and the availability of data. If no sufficient data is collected to provide an estimation for the preferred level of accuracy before the time deadline, the service shall return a zero confidence. Otherwise, the NWDAF may wait until enough data is collected before providing a response or a first notification.

- In order to be prepared for future requests on analytics from NFs/OAM, the NWDAF, upon operator configuration, may collect data on its own initiative, e.g. on samples of UEs, and retain the data collected in the data storage.

NOTE 1: The NWDAF can send an error response to the analytics consumer to indicate that statistics are unavailable if the NWDAF was not prepared for future requests and did not collect data on its own initiative.

The volume and maximum duration of data storage is also subject to operator configuration.

The NWDAF may decide to reduce the amount of data collected to reduce signalling load, by either prioritizing requests received from analytics consumers, or reducing the extent (e.g. duration, scope) of data collection, or modifying the sampling ratios. When using sampling ratio, the NWDAF may, depending on the analytics required and based on local configuration, provide additional partitioning criteria to the NFs to allow for a better UEs representation and to request that the NFs first partition the UEs before applying sampling ratio (see Event Reporting Information as specified in TS 23.502 [3]). The NWDAF may provide one or multiple partitioning criteria in its request for data collection from NFs.

The NWDAF may skip data collection phase when the NWDAF already has enough information to provide requested analytics.

The data which NWDAF may collect is listed for each analytics in input data clause and is decided by the NWDAF.

NOTE 2: NWDAF can skip data collection phase for some specific input data per the requested analytics e.g. when some of the data is already available at NWDAF for the requested analytics, or when NWDAF considers that some of the data is not needed at all to provide the requested analytics as per the analytics consumer request (e.g. based on preferred level of accuracy or based on the time when analytics are needed).

Event exposure subscriptions for data collection from the AMF and the SMF may need to survive after the removal of UE context in the AMF including event exposure subscriptions, or upon the creation of new UE context in AMF or SMF. In order for event exposure subscriptions in AMF and SMF to be (re)created in these cases, the NWDAF may subscribe to the events in AMF and/or SMF via UDM for a UE or group of UEs, as specified in TS 23.502 [3], clause 4.15.4.4.

In hierarchical interactions among NWDAFs, without standalone DCCF, or co-located DCCF, the efficiency of data collection can be achieved by inter-NWDAF instance cooperation among NWDAF instances on different levels of the hierarchy. An efficient data collection means that the same data required for the same Analytics ID or different Analytics IDs should not be collected multiple times by the different NWDAFs of the hierarchy.

6.2.2 Data Collection from NFs

6.2.2.1 General

The Data Collection from NFs is used by NWDAF to subscribe/unsubscribe at any 5GC NF to be notified for data on a set of events.

The Data Collection from NFs is based on the services of AMF, SMF, UDM, PCF, NRF and AF (possibly via NEF):

- Event Exposure Service offered by each NF as defined in TS 23.502 [3] clause 4.15 and clause 5.2.
- other NF services (e.g. Nnrf_NFDiscovery and Nnrf_NFManagement in NRF as defined in TS 23.502 [3] clause 4.17)

This data collection service is used directly in order to retrieve behaviour data for individual UEs or groups of UEs (e.g. UE reachability), and also to retrieve global UE information (e.g. Number of UEs present in a geographical area).

Table 6.2.2.1-1: NF Services consumed by NWDAF for data collection

Service producer	Service	Reference in TS 23.502 [3]
AMF	Namf_EventExposure (NOTE 3)	5.2.2.3 5.2.3.5
SMF	Nsmf_EventExposure (NOTE 3)	5.2.8.3 5.2.3.5
PCF	Npcf_EventExposure (for a group of UEs or any UE) Npcf_PolicyAuthorization_Subscribe (for a specific UE)	5.2.5.7
UDM	Nudm_EventExposure	5.2.3.5
NEF	Nnef_EventExposure	5.2.6.2
AF	Naf_EventExposure	5.2.19.2
NRF	Nnrf_NFDiscovery	5.2.7.3
	Nnrf_NFManagement	5.2.7.2

NOTE 1: The present document specifies that NWDAF can collect some UPF input data for deriving analytics, but how NWDAF collects these UPF input data is not defined in this Release of the specification.

NOTE 2: There is no data collected from the PCF by the NWDAF defined in this Release of the specification.

NOTE 3: The Nudm_EventExposure can be used when NWDAF uses the procedures specified in TS 23.502 [3] clause 4.15.4.4 to subscribe to AMF or SMF via UDM.

To retrieve data related to a specific UE, there are two cases:

- If no Area of interest is indicated by the consumer, the NWDAF shall first determine which NF instances are serving this UE as stated in table 6.2.2.1-2 unless the NWDAF has already obtained this information due to recent operations related to this UE.

- If an Area of interest is indicated, the NWDAF can:

  - First determine the AMF serving the UE and subscribe UE location from the AMF. Once the UE is in or moves into the Area of interest, the NWDAF determines which NF instances are serving this UE as stated in table 6.2.2.1-2 unless the NWDAF has already obtained this information due to recent operations related to this UE; or

  - Determine the NF instances of a given type of network function serving the Area of interest by querying NRF unless the NWDAF has already obtained this information due to recent operations related to this UE.

Table 6.2.2.1-2: NF Services consumed by NWDAF to determine which NF instances are serving a UE

Type of NF instance (serving the UE) to determine	NF to be contacted by NWDAF	Service	Reference in TS 23.502 [3]
UDM	NRF	Nnrf_NFDiscovery	5.2.7.3
AMF	UDM	Nudm_UECM	5.2.3.2
SMF	UDM	Nudm_UECM	5.2.3.2
BSF	NRF	Nnrf_NFDiscovery	5.2.7.3
PCF	BSF	Nbsf_Management	5.2.13.2
NEF	NRF	Nnrf_NFDiscovery	5.2.7.3
NWDAF	NRF UDM	Nnrf_NFDiscovery Nudm_UECM	5.2.7.3 5.2.3.2

The UDM instance should be determined using NRF as described in clause 4.17.4 of TS 23.502 [3] and factors to determine as described in clause 6.3.8 of TS 23.501 [2].

The AMF, SMF instances should be determined using a request to UDM providing the SUPI. To determine the SMF serving a PDU session, the NWDAF should in addition provide the DNN and S-NSSAI of this PDU Session; otherwise the NWDAF will obtain a list of possibly multiple SMFs (e.g. one per PDU session).

The BSF instance should be discovered using NRF thanks to optional request parameters (e.g. DNN list, IP domain list, IPv4 address range, IPv6 prefix range) as stated in clause 4.17.4 of TS 23.502 [3] or based on local configuration at the NWDAF.

The PCF instance serving UE PDU Session(s) should be determined using a request to BSF with the allocated UE address, DNN and S-NSSAI.

When NWDAF receives a request addressed to an Internal Group ID from a consumer, NWDAF may need to initiate data collection from several 5GC NFs, such as AMF, SMF, UDM, PCF, AF (e.g. via NEF), etc. If an Area of interest is indicated by the consumer, NWDAF may first discover the instances of the required 5GC NFs deployed in the network, e.g. by querying NRF, otherwise:

- For discovering the UDM, NWDAF can query the NRF with the Internal Group ID as the target of the query.
- For discovering AMF, SMF, PCF, NEF, and AF, NWDAF may need to discover all instances in the network by using the Nnrf_NFDiscovery service.

NOTE 4: It is assumed that all members of an Internal Group ID belong to the same UDM Group ID. NWDAF can select a UDM instance supporting the UDM Group ID of the Internal Group ID.

Then, if data needs to be collected from AMF, SMF, UDM, and PCF, NWDAF may initiate the data collection with the Internal Group ID as the target, e.g. subscribing to the event exposure in all the instances of a given type of network function. This subscription to all the instances of required source of event exposure handles, e.g. mobility of UEs across AMFs, or initiation of new PDU sessions with different allocated SMFs.

For collecting data from AMF and SMF, NWDAF may collect the data directly from AMF and/or SMF, or indirectly via UDM, according to TS 23.502 [3] clause 4.15.4.4. The indirect method may be required if the event exposure subscription from NWDAF, for a UE or group of UEs, needs to survive the removal of UE context in the AMF including event exposure subscriptions, or upon the creation of new UE context in AMF or SMF serving the UE or group of UEs. In this case the UDM is responsible for (re)creating event exposure subscriptions in AMF and SMF, as specified in TS 23.502 [3], clause 4.15.4.4.

The NWDAF determines to collect data from a trusted AF supporting specific Event ID(s) and serving specific application(s) based on internal configuration.

The NEF instance that is serving a specific network slices and/or applications of a UE should be determined using NRF using optional request parameters as defined in clause 6.3.14 of TS 23.501 [2]

If NWDAF needs to collect data from an AF deployed outside the operator's domain, the NWDAF shall contact NEF with a SUPI or Internal Group ID as the target of the data collection. NEF is responsible for translation of SUPI to GPSI, or internal to external group identifiers, by querying UDM, prior to contacting the AF.

NOTE 5: It is assumed that an AF is provisioned with the list of UE IDs (GPSIs or SUPIs) belonging to an External or Internal Group ID.

To retrieve required data for any UE, the NWDAF may subscribe to events from the AMF and/or SMF instances it has determined, setting the target of event reporting to "any UE" and the event filter(s) according to the Analytics Filter Information. Alternatively, if the required data is communication related and for any UE within an Area of interest, the NWDAF can obtain from the AMF instances it has determined a list of UEs located within the Area of Interest. Based on the obtained UE list, for each UE in the list, the NWDAF retrieves the SMF serving the UE and the NWDAF subscribes to data from the relevant SMF per each specific UE. The indirect event exposure subscription to AMF or SMF via UDM is not available for "any UE" or "any UE within an Area of interest". If the required data is collected from UE via AF as described in clause 6.2.8 and the Target of Analytics Reporting received from consumer is "any UE", the NWDAF may either set the target of event reporting to "any UE" in the data collection request to the AF, or may determine a list of UEs from AMF and/or SMF based on the Analytics Filter Information and send the data collection request to the AF for the determined list of UEs.

NOTE 6: If NWDAF requires collecting data from either AMF or SMF for "any UE" or "any UE within an Area of Interest", NWDAF can use the direct Event Exposure subscription to AMF or SMF, since subscriptions to "any UE" or "any UE within an Area of Interest" are persistent by nature in AMF or SMF, due to not being linked to a UE context.

To retrieve data related to "any UE" based on Analytics Filter Information, the NWDAF shall first determine which NF instances are matching the Analytics Filter Information (see clause 6.7.5.1) as stated in table 6.2.2.1-3 unless the NWDAF has already obtained this information due to recent operations related to this Analytics Filter Information.

Table 6.2.2.1-3: NF Services consumed by NWDAF to determine which NF instances are matching analytics filters

Type of NF instance (matching analytics filters) to determine	NF to be contacted by NWDAF	Service	Reference in TS 23.502 [3]
AMF, SMF	NRF	Nnrf_NFDiscovery	5.2.7.3

To retrieve data related to Analytics IDs for "any UE" with Analytics Filter Information defining an area of interest in terms of TA or Cells and/or with specific S-NSSAIs, NWDAF requires the network slice association information to properly determine the AMFs to collect data from as well as the proper queries to OAM for data collection.

NOTE 7: Examples of Analytics ID requiring NWDAF to use network slice association information for data retrieval are: network performance clause 6.6.1; user data congestion clause 6.8.1; QoS Sustainability clause 6.9; Dispersion Analytics clause 6.10.1; observed service experience for a Network Slice clause 6.4.1; and slice load analytics clause 6.3.

The network slice association information comprises the TAs associated with each AMF, and for each TAI its associated access type, cells and list of supported S-NSSAIs (including indication of S-NSSAIs restricted by AMF). Additionally, the mapping of cells per TAI and supported S-NSSAIs (including indication of S-NSSAIs restricted by AMF) for TAI for each AMF can change and NWDAF shall obtain this accurate information in order to properly retrieve data for analytics generation.

In order to derive the network slice association information, NWDAF may be configured with the mapping of cells per TAI, and the S-NSSAIs per TAI. NWDAF may subscribe to the "S-NSSAIs per TAI mapping" event exposed by AMF. The NWDAF may use the configured information (when the analytics subscription or request is at cell granularity) and the area of interest in the analytics subscription or request to retrieve from AMF the list of supported S-NSSAIs (including indication of S-NSSAIs restricted by AMF) per TAI, and access types per TAI for each AMF in the required area of interest. NWDAF consumes the "S-NSSAIs per TAI mapping" event exposed by AMF using, as target of event reporting, the list of TAIs based on the area of interest received in the Analytics Filter Information or identified by the mapping of the Cells per TAI matching to the Cell granularity included in the Analytics Filter Information. The AMF "S-NSSAIs per TAI mapping" event output contains, for each of the TAIs requested by NWDAF, its associated access type and the list of supported S-NSSAIs (including indication of S-NSSAIs restricted by AMF).

To retrieve data from SMFs for Analytics IDs subscription or requests for "any UE" including Analytics Filter Information with specific Applications, DNNs, DNAIs and area of interest per TA granularity, NWDAF shall first discover the SMF serving the area of interest via NRF.

NOTE 8: Examples of Analytics ID requiring NWDAF to collect data related to PDU sessions associated with an AoI with TA granularity are: network performance clause 6.6.1; user data congestion clause 6.8.1, QoS Sustainability clause 6.9.

NWDAF may directly consume events from the discovered SMF using the event target set to "any PDU session", and event filters with the same parameters of the Analytics Filter Information, i.e. list of Application IDs, and/or DNNs, and/or DNAI, and the area of interest related to the requested Analytics ID.

1. When SMF supports the exchange of UE Location parameter when SMF interacts with AMF via Nsmf_PDUSession_Create/Update/CreateSMContext/UpdateSMContext due to session establishment, modification, or release, service request, or handover procedures (as defined in the TS 23.502 [3] clause 5.2.8.2), SMF can directly map the PDU sessions to an AoI with TA granularity.

   If there are any changes in PDU sessions in the area of interest, for the Application ID, and/or DNN, and/or DNAI subscribed by NWDAF, SMF notifies the detected changes to NWDAF via Nsmf_EventExposure_Notify service operation, enabling NWDAF to keep an updated map of SMF and PDU sessions associated with the Analytics Filter Information in an area of interest.

2. When SMF does not support the exchange of UE Location parameter when SMF interacts with AMF but supports the mapping of PDU sessions per TA (as defined in TS 23.501 [2] clause 5.6.11), SMF may subscribe to UE mobility event notifications of AMF as described in clause 5.3.4.4 of TS 23.501 [2] using event ID "UE moving in or out of Area of Interest" and Event Filters as described in Table 5.2.2.3.1-1 from TS 23.502 [3] to retrieve the list of SUPIs (and GPSIs if available) in the area of interest. Based on the retrieved list of SUPIs in the area of interest, SMF identifies the PDU sessions in the area of interest.

3. When SMF does not support the exchange of UE Location parameter when SMF interacts with SMF nor supports the mapping of PDU sessions per TA (as defined in TS 23.501 [2] clause 5.6.11), SMF rejects the request from NWDAF. Upon the reject, NWDAF identifies the need to create the mapping of PDU sessions per TA. NWDAF subscribes to UE mobility event notifications of AMF as described in clause 5.3.4.4 of TS 23.501 [2] using event ID "UE moving in or out of Area of Interest" and Event Filters as described in Table 5.2.2.3.1-1 from TS 23.502 [3] to retrieve the list of SUPIs (and GPSIs if available) in the area of interest. Based on the retrieved list of SUPIs in the area of interest, NWDAF subscribes to the SMFs serving the UEs in the area of interest and derives the mapping of PDU sessions per TA.

An NWDAF may require to discover and select other NWDAFs for UE related analytics. In this case, the NWDAF may discover from UDM if an NWDAF is already collecting data related to the UE, as specified in clauses 5.2 and 6.1C.

6.2.2.2 Procedure for Data Collection from NFs

The procedure in Figure 6.2.2.2-1 is used by NWDAF to subscribe/unsubscribe at NFs in order to be notified for data collection on a related event (s), using Event Exposure Services as listed in Table 6.2.2.1-1. Depending on local regulation requirements, user consent for UE related data collection and usage of collected data may be required. User consent is defined for a specific purpose such as, e.g. analytics or model training. NWDAF checks user consent taking the purpose for data collection and usage of these data into account.

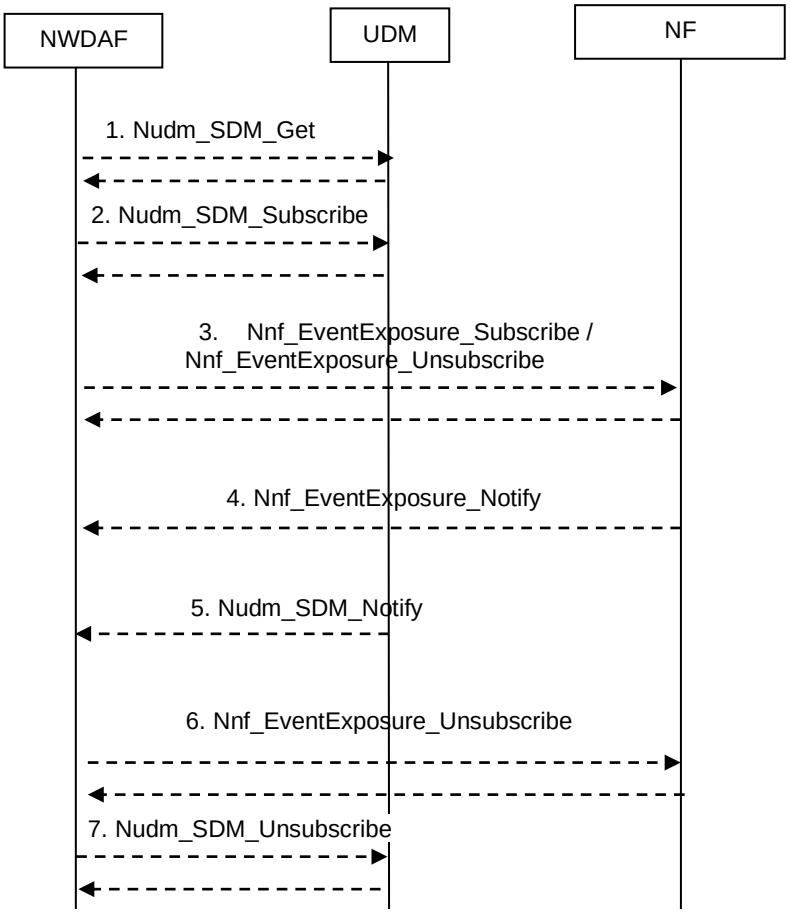

Figure 6.2.2.2-1: Event Exposure Subscribe/unsubscribe for NFs

1. The NWDAF checks if data is to be collected for a user, i.e., SUPI or GPSI, then, depending on local policy and regulations, the NWDAF checks the user consent by retrieving the user consent information from UDM using Nudm_SDM_Get including data type "User consent". If user consent is not granted, NWDAF does not subscribe to event exposure for events related to this user and the data collection for this SUPI or GPSI stops here.

2. If the user consent is granted, the NWDAF subscribes to UDM to notifications of changes on subscription data type "User consent" for this user using Nudm_SDM_Subscribe.

3. The NWDAF subscribes to or cancels subscription for a (set of) Event ID(s) by invoking the Nnf_EventExposure_Subscribe/Nnf_EventExposure_Unsubscribe service operation.

NOTE 1: The Event ID(s) are defined in TS 23.502 [3].

4. If NWDAF subscribes to a (set of) Event ID(s), the NFs notify the NWDAF (e.g. with the event report) by invoking Nnf_EventExposure_Notify service operation according to Event Reporting Information in the subscription.

   When the Reporting type is provided at step 1, the NWDAF determines that the events are disappeared, if the same events are included in the notification compared to the previous notification. Otherwise, NWDAF determines the events are newly appeared or changed. Also, the NWDAF restores the events that are not included in the notification, but included in the previous notification.

   If the Granularity of dynamics is applied to the subscription, the NWDAF shall infer the events in the NF from the events in the previous notification with the applied Granularity of dynamics.

NOTE 2: The Event Reporting Information are defined in TS 23.502 [3].

NOTE 3: The NWDAF can use the immediate reporting flag as defined in Table 4.15.1-1 of TS 23.502 [3] to meet the request-response model for data collection from NFs.

NOTE 4: This procedure is also used when the NWDAF subscribes for data from a trusted AF.

5. The UDM may notify the NWDAF on changes of user consent at any time after step 2.

6-7. If user consent is no longer granted for a user for which data has been collected, the NWDAF shall unsubscribe to any Event ID to collect data for that SUPI or GPSI. The NWDAF may unsubscribe to be notified of user consent updates from UDM for each SUPI for which data consent has been revoked.

6.2.2.3 Procedure for Data Collection from AF via NEF

The procedure in Figure 6.2.2.3-1 is used by NWDAF to collect information from AFs via the NEF.

NOTE 1: In this release, AF registers its available data to NWDAF via OAM configuration at NEF.

The AF collectable data information includes: AF identification, AF service identification (e.g. endpoint information of Naf_EventExposure), available data to be collected per application (e.g. identified by Event ID(s)).

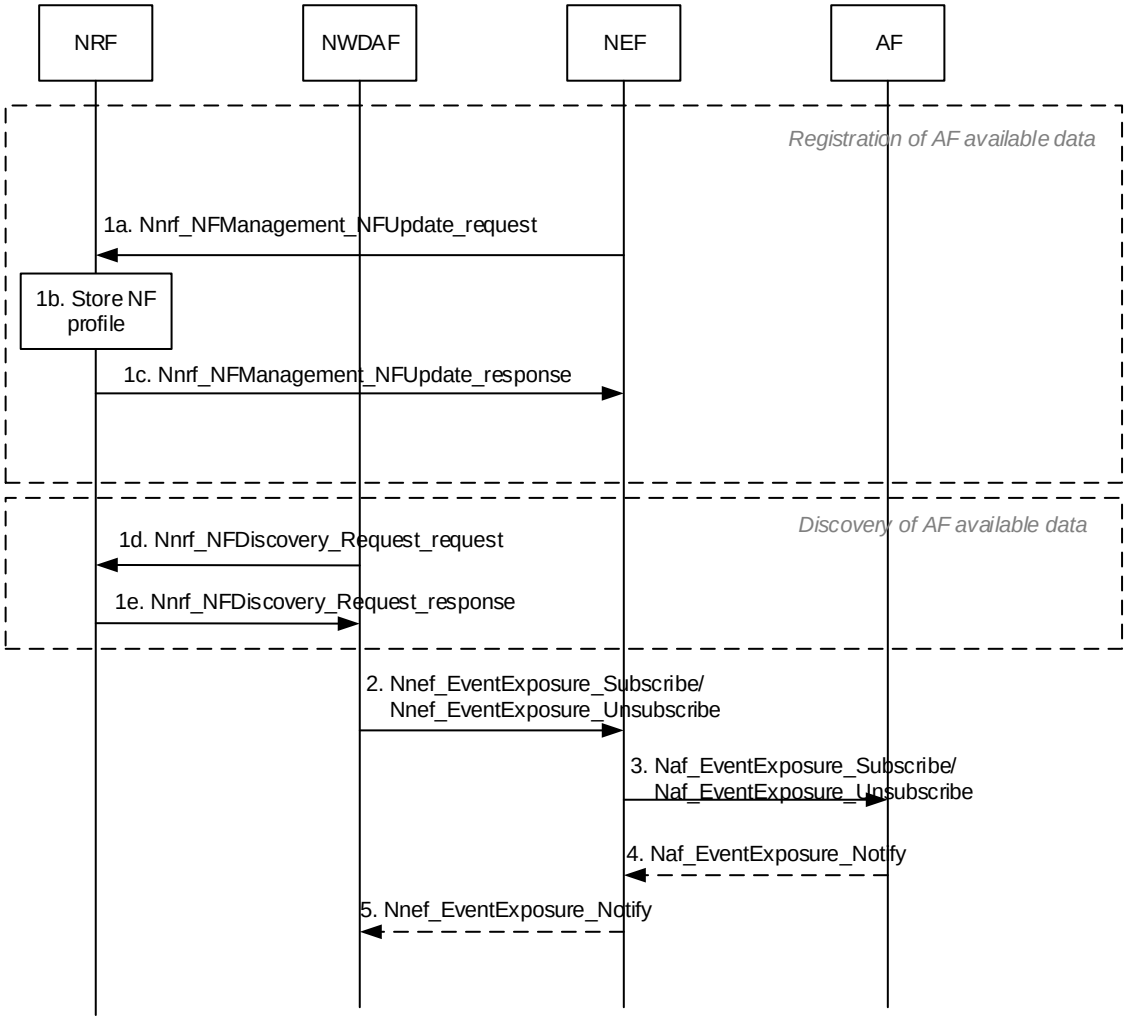

Figure 6.2.2.3-1: Data Collection from AF via NEF

1a. After the registration of AF available data at the NEF, NEF generates an event exposure with new EventID to be associated with available data to be collected from AF. NEF invokes Nnrf_NFManagement_NFUpdate_request service operation to update its registration information (i.e. NEF Profile) including the generated Event IDs, and associated AF identification, Application ID(s) (i.e. internal application ID or Application ID known in the core network).

1b. NRF stores the received NEF registration information including available data to be collected from AF.

1c. NRF sends Nnrf_NFManagement_NFUpdate_response message to NEF.

1d. When NWDAF needs to discovery the available data from AFs and the appropriated NEF to collect this data, NWDAF invokes Nnrf_NFDiscovery_Request_request service operation using as parameter the NEF NF Type, a list of Event ID(s), and optionally AF identification, application ID.

1e. NRF matches the requested query for available data in AFs with the registered NEF Profiles and sends this information via Nnrf_NFDiscovery_Request_response message to NWDAF.

NOTE 2: After the registration and discovery procedure described in step 1, NWDAF identifies the available data per AF per application and the proper NEF to collect such data.

2. The NWDAF subscribes to or cancels subscription to data in AF via NEF by invoking the Nnef_EventExposure_Subscribe or Nnef_EventExposure_Unsubscribe service operation. If the event subscription is authorized by the NEF, the NEF records the association of the event trigger and the NWDAF identity.

NOTE 3: User consent for retrieving user data in AF via NEF is not specified in this Release.

3. Based on the request from the NWDAF, the NEF subscribes to or cancels subscription to data in AF by invoking the Naf_EventExposure_Subscribe/ Naf_EventExposure_Unsubscribe service operation.

4. If the NEF subscribes to data in AF, the AF notifies the NEF with the data by invoking Naf_EventExposure_Notify service operation according to Event Reporting Information in the subscription.

5. If the NEF receives the notification from the AF, the NEF notifies the NWDAF with the data by invoking Nnef_EventExposure_Notify service operation.

   When the Reporting type is provided at step 2, the NWDAF determines that the events are disappeared, if the same events are included in the notification compared to the previous notification. Otherwise, NWDAF determines the events are newly appeared or changed. Also, the NWDAF restores the events that are not included in the notification, but included in the previous notification.

   If the Granularity of dynamics is applied to the subscription, the NWDAF shall infer the events in the AF from the events in the previous notification and the applied Granularity of dynamics.

6.2.2.4 Procedure for Data Collection from NRF

The NWDAF may use NRF services and Network Function service framework procedures as defined in TS 23.502 [3] clause 5.2.7 and clause 4.17:

- NF/NF service discovery procedures (in TS 23.502 [3] clause 4.17.4) and Nnrf_NFDiscovery service (in TS 23.502 [3] clause 5.2.7.3) in order to dynamically discover the NF instances and services of the 5GC. Such discovery may be performed on a periodic basis, or under specific circumstances.

- NF/NF service status subscribe/notify procedures (in TS 23.502 [3] clause 4.17.7) and Nnrf_NFManagement service (in TS 23.502 [3] clause 5.2.7.2) in order to be notified about the change of status of an NF. The service operations for obtaining status information are NFStatusSubscribe and NFStatusNotify, from the Nnrf_NFManagement service.

The information provided by the NRF to the NWDAF with the Nnrf_NFDiscovery_Request and the Nnrf_NFManagement_NFStatusNotify service operations are the NF Profiles and the NF services as defined in TS 23.502 [3] clause 5.2.7. Such information can be used to set-up and maintain a consistent network map for data collection and also, depending on use cases, to perform analytics (e.g. NF load analytics as defined in clause 6.5).

If the NWDAF needs to keep a consistent network map for data collection from AMFs and SMFs associated with a list of TAs, the subscription to NFStatusSubscribe for such type of NFs may include the list of TAs target.

6.2.2.5 Usage of Exposure framework by the NWDAF for Data Collection

The NWDAF shall subscribe (and unsubscribe) to the Event exposure service from NF(s) reusing the framework defined in TS 23.502 [3] clause 4.15. This framework supports the possibility for the NWDAF to indicate/request:

- Events-ID: one or multiple Event ID(s) defined in TS 23.502 [3] clause 4.15.1

- Target of Event Reporting defined in TS 23.502 [3] clause 4.15.1: the objects targeted by the Events. Within a subscription, all Event ID(s) are associated with the same target of event reporting. In the case of NWDAF, the objects can be UE(s), UE group(s), any UE.

- Event Filter Information defined in TS 23.502 [3] clause 4.15.1. This provides Event Parameter Types and Event Parameter Value(s) to be matched against.

- A Notification Target Address and a Notification Correlation ID as defined in TS 23.502 [3] clause 4.15.1, allowing the NWDAF to correlate notifications received from the NF with this subscription.

- Event Reporting Information described in TS 23.502 [3] Table 4.15.1-1 and the muted stored events exposure as described in clause 6.2.7.

- Expiry time as defined in TS 23.502 [3] clause 4.15.1.

The notifications from NFs/AFs contain on top of the Event being reported (and of dedicated information being reported for this event):

- the Notification Correlation Information provided by the NWDAF in its request,
- (when applicable to the event) the Target Id e.g. UE ID (SUPI and if available GPSI), and
- a time stamp.

6.2.3 Data Collection from OAM

6.2.3.1 General

The NWDAF may collect relevant management data from the services in the OAM as configured by the PLMN operator.

- NG RAN or 5GC performance measurements as defined in TS 28.552 [8].
- 5G End to end KPIs as defined in TS 28.554 [10].

NWDAF shall use the following services to have access to the information provided by OAM:

- Generic performance assurance and fault supervision management services as defined in TS 28.532 [6].
- PM (Performance Management) services as defined in TS 28.550 [7].
- FS (Fault Supervision) services defined in TS 28.545 [9].

Editor's note: The MDA services are to be defined by SA WG5 and NWDAF could subscribe to them. The reference to SA WG5 specification will be added when defined in SA WG5.

NWDAF can be configured to invoke the existing OAM services to retrieve the management data that are relevant for analytics generation, which may include NF resources usage information (e.g. usage of virtual resources assigned to NF) and NF resource configuration information (e.g. life cycle changes of NF resource configurations).

OAM perform the required configuration in order to provide the information requested by NWDAF subscription and perform the tasks, e.g. data collection, data processing, associated with the subscribed request from NWDAF.

Another usage of OAM services is when the target of data collection is a specific UE, via MDT based retrieval of information:

- Measurement collection for MDT as defined in TS 37.320 [20].

In addition, NWDAF can be provisioned with Network Slice information (i.e. as defined by the NetworkSliceInfo specified in TS 28.541 [22]) when a slice is created or modified via OAM configuration mechanism as defined in TS 28.541 [22] and TS 28.532 [6].

6.2.3.2 Procedure for data collection from OAM

The interactions between NWDAF and OAM for data collection are illustrated in Figure 6.2.3.2-1. The data collected depends on the use cases. This figure is an abstraction of the OAM performance data file report management service that is defined TS 28.532 [6]. The actual OAM services and reporting mechanisms that NWDAF may use are specified in TS 28.532 [6], TS 28.550 [7] or TS 28.545 [9].

The flow below assumes the NWDAF is configured on how to subscribe to the relevant OAM services.

OAM shall setup the required mechanisms to guarantee the continuous data collection requested by NWDAF.

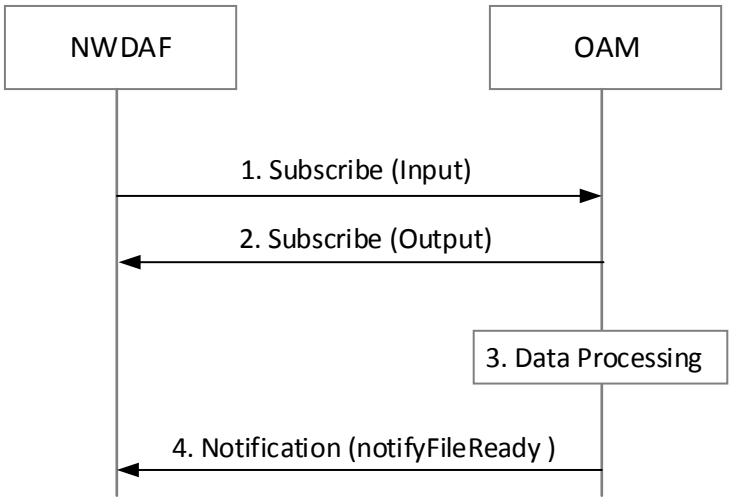

Figure 6.2.3.2-1: Data collection from OAM performance data file report management service

1. (Clause 11.3.1.1.3.2 ofTS 28.532 [6]), Subscribe (Input): NWDAF subscribes to the notification(s) related to the services provided by the management service producer.

2. (Clause 11.3.1.1.3.3 ofTS 28.532 [6]), Subscribe (Output): management service producer responses to NWDAF if the subscription is success or not.

3. Data processing: management service producer prepares the data.

4. (Clause 11.3.1.1.1 ofTS 28.532 [6]), Notification (notifyFileReady): management service producer notifies the data file is ready.

As the final step, NWDAF fetches data by using FTP (not specified in 3GPP, based on vendor implementation).

NOTE 1: The call flow in Figure 6.2.3.2-1 only shows a subscribe/notify model for the simplicity, however both request-response and subscription-notification models are supported.

NOTE 2: NWDAF is configured with the Network Slice information (i.e. NetworkSliceInfo including a DN (Distinguished Name) of the NetworkSlice managed object relating to the network slice instance associated to the S-NSSAI and NSI ID if available as defined in TS 28.541 [22]). Based on the Network Slice information, the NWDAF uses the DN (Distinguished Name) to identify the NetworkSlice managed object relating to the S-NSSAI and NSI ID and consumes the management services to collect the management data of the corresponding NetworkSlice managed object (including the NRF serving the network slice, the NFs associated to the network slice, the NG RAN or 5GC performance measurements defined in TS 28.552 [8], or the 5G end to end KPIs defined in TS 28.554 [10]) provided by OAM.

6.2.4 Correlation between network data and service data

The Correlation information in input data which helps NWDAF correlate data from different NFs, OAM and UE application(s) is defined in Table 6.2.4-1, which is subject to all the network data analytics.

NOTE: For simplicity, the correlation information is not listed in the input data per network data analytics.

Table 6.2.4-1: Correlation Information

Correlation Information	Description
Timestamp, IP address 5-tuple	To correlate the data from AF and from UPF.
Timestamp, AN Tunnel Info (Clause 9.3.2.2 of TS 38.413 [16])	To correlate the UPF data and OAM data which are reported by the RAN (e.g. Reference Signal Received Power or Reference Signal Received Quality as defined in Table 6.4.2-3).
Timestamp, UE IP address	To correlate the data from UPF and SMF.
Timestamp, SUPI	To correlate data from SMF and AMF.
Timestamp, SUPI,DNN, S-NSSAI or UE IP address	To correlate data from SMF and PCF.
Timestamp, RAN UE NGAP ID (Clause 9.3.3.2 of TS 38.413 [16]) and Global RAN Node ID	To correlate the AMF data and OAM data reported by the RAN (e.g. Reference Signal Received Power or Reference Signal Received Quality as defined in Table 6.4.2-3).
Timestamp, Application ID, IP filter information	To correlate data from SMF and AF.
Timestamp, UE ID or UE IP address, Application ID, DNN, S-NSSAI	To correlate data from 5GC NF (e.g. SMF, UPF) and UE Application (via the AF).

6.2.5 Time coordination across multiple NWDAF instances

6.2.5.1 General

In certain situations, an NWDAF Service Consumer expects to receive analytics by a given time. In particular, when an NWDAF Service Consumer is collecting analytics from multiple NWDAFs it can be necessary to coordinate the timing of the analytics subscriptions/requests from the same NWDAF service consumer.

The NWDAF Service Consumer may use "time when analytics information is needed parameter" (see clause 6.1.3) as a dynamic timer to indicate the minimum time it is going to wait (i.e. "expected waiting time") to receive the analytics collected from multiple NWDAFs.

6.2.5.2 Procedure for time coordination across multiple NWDAFs

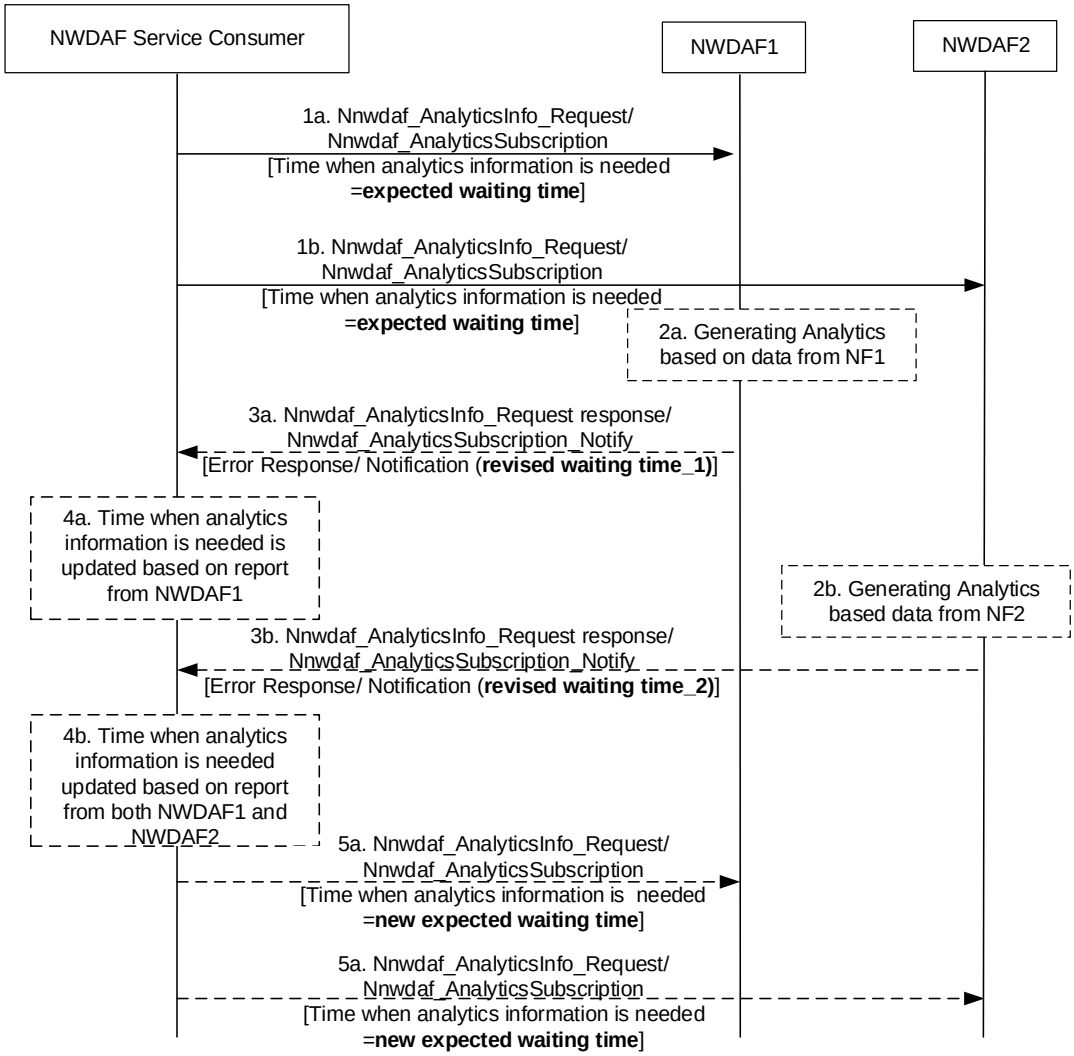

Figure 6.2.5.2-1: Procedure for time coordination across multiple NWDAFs

1a-1b. On analytics request/subscription, the NWDAF Service Consumer indicates the "expected waiting time" as "time when analytics is needed" parameter to those NWDAFs from which it expects to receive the analytics latest by the "time when analytics information is needed", using either the Nnwdaf_AnalyticsInfo_Request or Nnwdaf_AnalyticsSubscription_Subscribe service operation. In this example, NWDAF1 and NWDAF2 are the NWDAFs with tightly related analytics.

2a-2b. Each NWDAF generates the requested analytics based on data from related data sources. In this example, NWDAF1 processes data from NF1 and NWDAF2 processes data from NF2.

3a-3b. [Optional] If the "time when analytics information is needed" is reached, but the analytics is not ready, the NWDAF may indicate a "revised waiting time" in an error response or error notification, using either the Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify service operation, depending on the service used in step 1.

4a-4b. [Optional] On receiving an indicated "revised waiting time" as part of an error response or error notification, the NWDAF Service consumer may use the "revised waiting time" to update the "time when analytics information is needed" parameter for future analytics requests/subscriptions to the same group of NWDAFs.

5a-5b. If the value of the "time when analytics information is needed" was updated in step 4, the NWDAF Service Consumer, in future requests or within current subscription, indicates the new expected waiting time as "time when analytics information is needed" to all NWDAFs with tightly related analytics, using either the Nnwdaf_AnalyticsInfo_Request or Nnwdaf_AnalyticsSubscription_Subscribe service operation.

NOTE 1: Steps 3a-3b and steps 4a-4b may happen in different orders depending on the timing of analytics collection (from other NFs, e.g. NF1 or NF2) or processing.

NOTE 2: Parameter "time when analytics is needed" as in steps 1a-1b, 3a-3b, 4a-4b and 5a-5b can be per individual Analytics ID.

6.2.6 Enhanced Procedures for Data Collection

6.2.6.0 General

Data collection may be performed via DCCF, MFAF and ADRF, when such NFs are deployed, or via NWDAF (hosting DCCF and/or ADRF). The NF services used for DCCF, MFAF, ADRF and the NWDAF (hosting DCCF and/or ADRF) are listed in Table 6.2.6.0-1.

Table 6.2.6.0-1: NF Services for the enhanced data collection procedures

Service producer	Service	Reference
NWDAF	Nnwdaf_DataManagement	7.4
DCCF	Ndccf_DataManagement Ndccf_ContextManagement	8.2 8.3
MFAF	Nmfaf_3daDataManagement Nmfaf_3caDataManagement	9.2 9.3
ADRF	Nadrf_DataManagement	10.2

DCCF, MFAF, and NWDAF hosting DCCF shall use the same services listed in clause 6.2.1 from OAM, and NFs (including AFs directly or via NEF) to collect data. Additionally, the new services for data exposure from DCCF, MFAF, ADRF and NWDAF (hosting DCCF and/or ADRF) as specified in clause 8, 9, 10 and 7.4 may also be used for data collection.

The NWDAF, DCCF, ADRF shall obtain the proper information to perform data collection for a UE, a group of UEs or any UE following the principles of clause 6.2.1.

When NWDAF or DCCF need to discover the sources of data collection, they follow the principles defined in clause 6.2.2.1 in the case of data collection from NFs; in clause 5A.2 in the case of DCCF deployed in the network and requiring data from NWDAFs or ARDFs that independently collect data; clause 5.2 in the case of NWDAF (hosting DCCFs) and collecting data from other NWDAFs.

6.2.6.1 Bulked Data Collection

6.2.6.1.0 General

NWDAFs or DCCF or MFAF or ADRF may provide bulked data to consumers as an alternative to providing individual events (i.e. subscription to multiple event IDs to obtain the data required for an analytics generation).

The bulked data is the set of data samples from the collected event notifications to be used for an Analytics ID for a consumer of NWDAF, DCCF, MFAF or ADRF. A data sample may be a notification, in which case the bulked data may comprise a group of received notifications, or a data sample may be information extracted from a notification and processed, in which case the bulked data comprises the processed information. The bulked data can be used for the purpose of analytics inference or ML model training.

The bulked data is generated based on the set of data samples from event notifications collected from NFs/OAM and the properties for the selection of such data, Consumers of bulked data or operators may define different rules (e.g. aggregation formats or processes) for generation of bulked data for training or inference.

NFs capable to expose bulked data have the following capabilities:

- Exposing runtime collected data (e.g. data from NFs/AFs/OAM retrieved via notification mechanisms), or historical collected data (e.g. data from NFs/AFs/OAM that were at some point collected, then stored), or both;

- Applying selection processes of data samples or processing mechanisms for the generation of the bulked data according to bulked data formatting and processing instructions provided by consumers of the bulked data or defined by an operator. The bulked data formatting and processing instructions may include the formatting and

processing instructions as specified in clause 5A.4 and further instructions as described in clause 6.2.6.1.1. Such instructions define the allowed and/or restricted properties and/or processes to be applied to the set of data from the collected event notifications to be used for the bulked data, the properties and processes being:

- The properties associated with the Bulked data formatting and processing are filters over the data to be associated with the bulked data. The properties for bulked data are defined as per Data Specification parameters in clause 6.2.6.1.1.

- The processes associated with the bulked data formatting and processing are mechanisms applied to the data to be associated with the bulked data and are defined according to the Formatting and Processing parameter defined in clause 5A.4 and the further instructions defined in clause 6.2.6.1.1. These processes may comprise: definition if data to be used for composing the bulked data is directly extracted from collected events, or the data is extracted from event notification of the same event type and pre-processed, or both; applying anonymization of data fields in the bulked data to avoid exposing undesired information, aggregation levels (i.e. per cell, per UEs, or temporal, e.g. per hours or days).

NOTE: Pre-process data from collected event notifications of the same event type refers to the usage of data manipulation processes in order to aggregate, concatenate, process data from multiple collected event notifications from the same event type that results in a single processed value.

- Having the mapping of the Service Operation that have to be used for collecting data of the bulked data associated with an Analytics ID.

6.2.6.1.1 Services for Bulked Data Collection

NWDAF, DCCF, MFAF, ADRF may expose service(s), respectively, the Nnwdaf_DataManagement_Subscribe or Ndccf_DataManagement_Subscribe, Nmfaf_3daDataManagement_Configure, Nadrf_DataManagement_RetrievalSubscribe service operation with a request for bulked data including the following input parameters:

- Data Specification:

  - Event ID(s) or Analytics ID(s);

    - In the case of Event IDs, the Data Specification fields includes the fields Target of Event Reporting and Event Filter Information as defined in TS 23.502 [3] clause 4.15.1, and Bulked Data Type parameter, which can be set to "raw data samples" (i.e. data is directly extracted from collected events) or "pre-processed data samples" (i.e. data from collected events is processed and the processed data is included in the bulked data) or a combination of both;

    - If the Analytics ID(s), the Data Specification fields contain:

      - Target of Reporting including a tuple with Analytics ID; Bulked Data Type, which can be set to "raw data samples" (i.e. data is directly extracted from collected events) or "pre-processed data samples" (i.e. data from collected events is processed and the processed data is included in the bulked data) or a combination of both; analytics stage (inference or training);

      - Filter Information may include fields related to the Analytics ID such as: Target of Analytics Information (e.g. any UE, list of UEs, groups of UEs); Analytics Filter Information (e.g. area of interest, DNN, Application, S-NSSAI). The Analytics ID also determines the Service Operation from NFs, OAM to be used and type of data (i.e. Event IDs, OAM measurements) to be collected and associated with the bulked data.

- Service Operation in the case of Event ID, defines the service operation to be used by NWDAF, DCCF, MFAF, or ADRF to request data (e.g. Namf_EventExposure_Subscribe or OAM Subscribe)

- Bulked Data Formatting and Processing: the parameters defined in TS 23.502 [3] clause 4.15.1 for Event Reporting Information and Formatting and Processing as defined in clause 5A.4 may be part of the possible formatting and processing instructions to be applied for bulked data generation. Additionally, the following parameters may be also included:

  - Periodic bulked data notification: Notifications are sent periodically (e.g. every hour) and may also in a specified time window (e.g. 2AM to 3AM), irrespective of the number of notifications from a Data Source or amount of data that have been bulked. Applicable when the Fetch Flag=false.

- Feature type is the field defining the type of pre-processing to be applied to the data from the collected event notifications if the bulked data type includes "pre-processed data samples". In this case, for each feature type there is an associated list of events that should be processed according with the feature type. Feature types are: average, maximum, minimum, skewed value from the collected event notification, most frequent value, and least frequent value.

NOTE: The desired feature type needs to be compatible with the possible processing applicable to the event notifications of the Event ID.

- Time Window: Specifies the start and stop time for the requested data or analytics.
  - If the Time Window includes a period in the past, then the data or analytics collection is "historical".
  - If the Time Window includes a period in the future, the data or analytics collection is "runtime".
- (Optional) Minimum and/or maximum number of samples to be included in the bulked data.
- Fetch flag, when set to false, it indicates that the bulked data needs to be generated and included in notification messages; when set to true, it indicates that bulked data will not be returned in the notification messages and the consumer must fetch the bulk data. The default value of fetch flag is false.
- Bulked data deadline, which indicates the limit of time for the consumer to fetch bulked data after receiving a notification that the data is available. Applicable when the fetch flag is set to true.
- Notification Event Clubbing as defined in clause 5A.4, indicates the number of notifications from a data source to be bulked before sending a notification containing the bulked data to the Consumer. Applicable when the Fetch Flag=False.
- Processing rules: the types of data manipulation to be applied for the requested bulked data and comprises:entity or geographical aggregation level (e.g. per UEs, per AoI), temporal aggregation (i.e. per minute, per hour); anonymization rules (e.g. anonymization of UE identifications).

- A Notification Target Address (+ Notification Correlation ID), where the Notification Correlation ID is the unique identification for the bulked data being generated for the requesting consumer.
- ADRF ID or NWDAF ID (or ADRF Set ID or NWDAF Set ID) storing historical data (optional). If known to the consumer, this may be specified to direct a DCCF or an NWDAF to the repository containing historical data.
- (Optional) ADRF information indicating whether the collected data for the generation of the bulked data are to be stored in an ADRF, and optionally an ADRF ID.
- (Optional, in case the requested data is Event IDs) Data Source identification to collect the data, e.g. NF Instance (or NF Set) ID from which the data needs to be collected.

The output parameter of the Nnwdaf_DataManagement_Subscribe or Ndccf_DataManagement_Subscribe, or Nadrf_DataManagement_RetrievalSubscribe service operation comprise the subscription correlation ID, which identifies the requested bulked data.

The input parameters of Nnwdaf_DataManagement_Notify or Ndccf_DataManagement_Notify, or Nmfaf_3caDataManagement_Notify, or Nadrf_DataManagement_RetrievalNotify service operation shall contain the Notification Correlation ID, and the generated bulked data when the fetch flag = false. When the fetch flag = true the notifications will contain the Notification Correlation ID, the Fetch Correlation ID and a target address where the generated bulked data may be retrieved. In the case of unsuccessful bulked data generation, the notification will contain an indication of an unsuccessful bulked data generation, optionally with expired bulked data deadline.

The input parameters for the service operation Nnwdaf_DataManagement_Fetch or Ndccf_DataManagement_Fetch, or Nmfaf_3caDataManagement_Fetch, or Nadrf_DataManagement_RetrievalRequest include: the Notification correlation ID (+list of Fetch Correlation ID), which identifies the requested bulked data.

The output parameters for the service operation Nnwdaf_DataManagement_Fetch include:

- the generated bulked data.

The generated bulked data exposed by the above listed service operations comprises:

- the dataset (i.e. the resulting set of data samples and/or set of pre-processed data samples from the collected event notifications) generated based on the parameters of bulked data request and instructions for bulked data generation, with each data sample including the following data structure:
  - if the bulked data type is "pre-processed data samples" the data type (e.g. Event ID) and associated feature type (e.g. average values of Event ID) are included;
  - data value (when "data samples" bulk data type is used) or processed values (when "pre-processed data samples" bulked data type is used);
  - timestamp when the data sample is associated with a bulked data.

6.2.6.2 Procedure for Data Collection from NWDAF

The procedure in Figure 6.2.6.2-1 is used by NWDAF service consumer to invoke the data management services at NWDAFs in order to retrieve runtime and historical data.

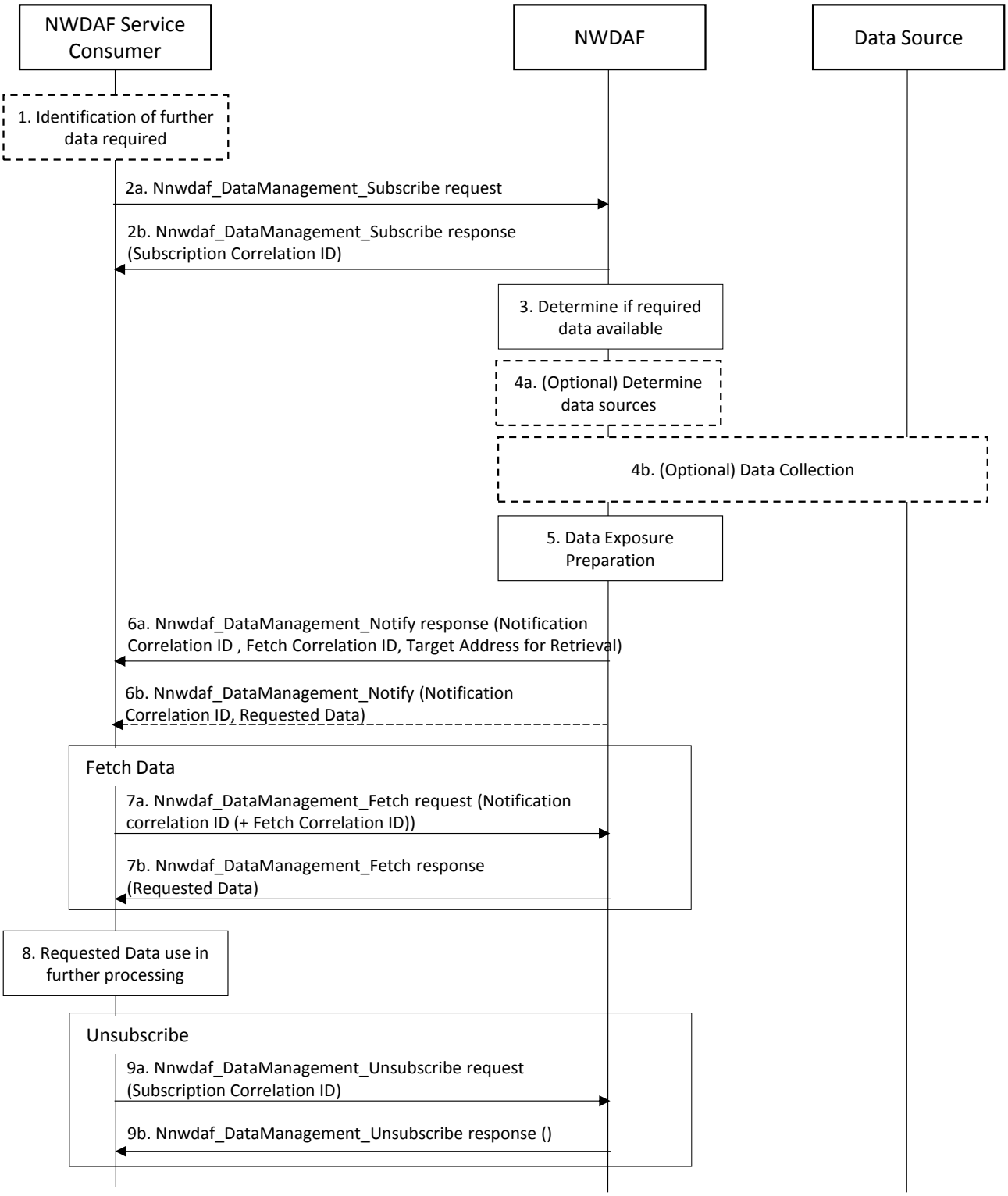

Figure 6.2.6.2-1: Data Collection from NWDAF via Data Management Service

1. NWDAF service consumer (e.g. NWDAF, DCCF) identifies that further data from an NWDAF is required in order to perform some operation related to Analytics ID. The triggers for further data collection are related to:

   a) the local policies of NWDAF or DCCF (e.g. preparation for future requests for Analytics ID as specified in clause 6.2.2.1);

   b) a request for analytics generation requiring data not available or not directly reachable via the NWDAF service consumer (e.g. out of the serving area);

   c) a request for model training;

d) a request for data collection that NWDAF service consumer cannot provide by itself.

NOTE 1: If the NWDAF service consumer is a DCCF, the discovery of the proper NWDAF is defined in clause 6.2.6.3.6. If the NWDAF service consumer is a NWDAF, the NWDAF service consumer can discover the appropriate NWDAF(s) as defined in clause 5.2.

2a. NWDAF service consumer invokes Nnwdaf_DataManagement_Subscribe service from NWDAF to request a required data. The request comprises the Data Specification as well as Bulked Data Formatting and Processing as defined in clause 6.2.6.1, Notification Target Address (+ Notification Correlation ID).

When the required data is Event IDs, the NWDAF service consumer may include the Data Source, e.g. NF Instance (or NF Set) ID from which the data needs to be collected.

The NWDAF service consumer may include ADRF information indicating whether the data are to be stored in an ADRF, and optionally an ADRF ID.

The NWDAF service consumer may include ADRF ID or NWDAF ID (or ADRF Set ID or NWDAF Set ID) storing historical data (optional), directing NWDAF to the repository containing historical data.

The NWDAF checks if required data is related to a user, i.e. SUPI or GPSI, then, depending on local policy and regulations, as described in clause 6.2.9, the NWDAF checks or has checked the user consent by retrieving the user consent information from UDM using Nudm_SDM_Get including data type "User consent". If user consent is not granted, NWDAF sends a response to the NWDAF service consumer in step 2b, indicating that user consent for data collection was not granted, and the data collection for this SUPI or GPSI stops here. If the user consent is granted, the NWDAF can provide the required data to the NWDAF service consumer by performing the following steps 2b-7, and the NWDAF subscribes to UDM to notifications of changes on subscription data type "User consent" for this user using Nudm_SDM_Subscribe. When receiving the notification that user consent has been revoked, the NWDAF shall provide a Termination Request in Nnwdaf_DataManagement_Notify to request the NWDAF service consumer to cancel the subscription to the required data.

2b. Based on the received request, NWDAF creates a new bulked data for the requesting consumer. NWDAF sends Nnwdaf_DataManagement_Subscribe service response with a confirmation of successful request and the subscription correlation ID identifying the requested data.

NOTE 2: Subscription Correlation ID allows the NWDAF service consumer to request to NWDAF any changes in the generation of a requested data.

3. NWDAF determines whether the request data is available at such NWDAF.

NWDAF maintains a local association of requested Event IDs or Analytics IDs to the list of triggered event subscription identifications from data sources to generate the requested data. Based on this local association, the NWDAF checks if the data to be collected is available at itself. If the data is available, NWDAF uses such data to generate the bulked data.

When data sources are NFs, the NWDAF discovers the proper NFs as defined in clause 6.2.2.1.

When the data sources are other NWDAFs, the NWDAF discovers the other NWDAFs as defined in clause 5.2.

When the data source is DCCF, the NWDAF discovers the proper DCCF as defined in clause 6.3.19 ofTS 23.501 [2].

4a. (Optional) If NWDAF receives a request for data that is not available or not reachable by such NWDAF (e.g. out of serving area), NWDAF determines the sources for the data that is not available, if the information has not been included in the subscription to the requested data.

4b. (Optional) NWDAF may trigger further data collection using any of the available mechanisms in clause 6.2.2 (e.g. if the data subscribed in step 2a partially matches data that are already being collected by the NWDAF from a data source and a modification of the subscription to the data source would satisfy both the existing data collection as well as the newly requested data) and clause 6.2.6 (e.g. recursively using data collection services from other needed NWDAFs, DCCFs, ADRFs, NFs).

NWDAF updates its local association of the mapping of the requested data (Event ID or Analytics ID) to the identification of the request/subscription for data collection from the further data sources.

5. Based on the properties of the received request and considering local bulked data instructions, NWDAF generates the requested data including the available or collected data (e.g. from other NWDAFs, DCCFs or ADRFs, NFs).

6a. If the fetch flag is set to true in step 2a, NWDAF waits until the requested data is ready and sends a Nnwdaf_DataManagement_Notify service message with the Notification Correlation ID, the Fetch Correlation ID and the target address where the data may be retrieved.

The requested data is ready when NWDAF generated the bulked data based on the available or collected data samples from the event notifications and the applicable bulked data processing and formatting instructions.

6b. If the fetch flag is set to false in step 2a, NWDAF uses the Nnwdaf_DataManagement_Notify service to send the Notification Correlation ID and requested data to the NWDAF service consumer.

NWDAF waits until the bulked data is generated or the bulked data deadline expires and uses Nnwdaf_DataManagement_Notify service with the indication of the outcome. In case of successful bulked data generation, NWDAF provides the bulked data via Nnwdaf_DataManagement_Notify service as defined in clause 6.2.6.1. In case of bulked data deadline expiration and unsuccessful bulked data generation, NWDAF provides the bulked data via Nnwdaf_DataManagement_Notify an indication of an unsuccessful bulked data generation with expired deadline. The Notification Target Address is used by the Nnwdaf_DataManagement_Notify service operation to deliver the message to the NWDAF service consumer.

7(a.b). Alternatively, when the fetch flag is set to true in Step 2a, the NWDAF service consumer shall fetch the required data from NWDAF via Nnwdaf_DataManagement_Fetch service operation. The NWDAF service consumer invokes the Nnwdaf_DataManagement_Fetch service operation with the input parameters including the Notification Correlation ID (+Fetch Correlation ID), that identifies the data to be fetched and receives a response with the requested data, as defined in clause 6.2.6.1.

8. The NWDAF service consumer uses the requested data for performing further processing. If the NWDAF service consumer is an NWDAF the requested data can be used for analytics generation or model training or for further exposing such data to other NWDAFs. If the NWDAF service consumer is a DCCF, the requested data can be used to be provided to a DCCF data consumer.

9. When the NWDAF service consumer determines that no more data is required or if receiving a Termination Request from the NWDAF, e.g. due to user consent revocation for the data collection related to a user, it unsubscribes to the requested data from NWDAF. If NWDAF had triggered further data collection in Step 3a and 3b, NWDAF also unsubscribe to all data sources.

NOTE 3: It is also possible that instead of providing the dataset of the generated bulked data in steps 6a, 6b, 7b, the NWDAF provides a reference to where the dataset can be retrieved by the NWDAF service consumer.

6.2.6.3 Data Collection using DCCF

6.2.6.3.1 General

This clause specifies procedures for data collection using the DCCF described in clause 5A for cases other than obtaining analytics from an NWDAF (which is specified in clause 6.1.2). Two options are supported: data delivered via the DCCF, according to clauses 6.2.6.3.2 and 6.2.6.3.3, and data delivered via a messaging framework according to clauses 6.2.6.3.4 and 6.2.6.3.5. Which option to be used is determined by DCCF configuration.

6.2.6.3.2 Data Collection via DCCF

The procedure depicted in Figure 6.2.6.3.2-1 is used by a data consumer (e.g. NWDAF) to obtain data and be notified of events via the DCCF using Ndccf_DataManagement_Subscribe service operation. Whether the data consumer directly contacts the Data Source or goes via the DCCF is based on configuration of the data consumer.

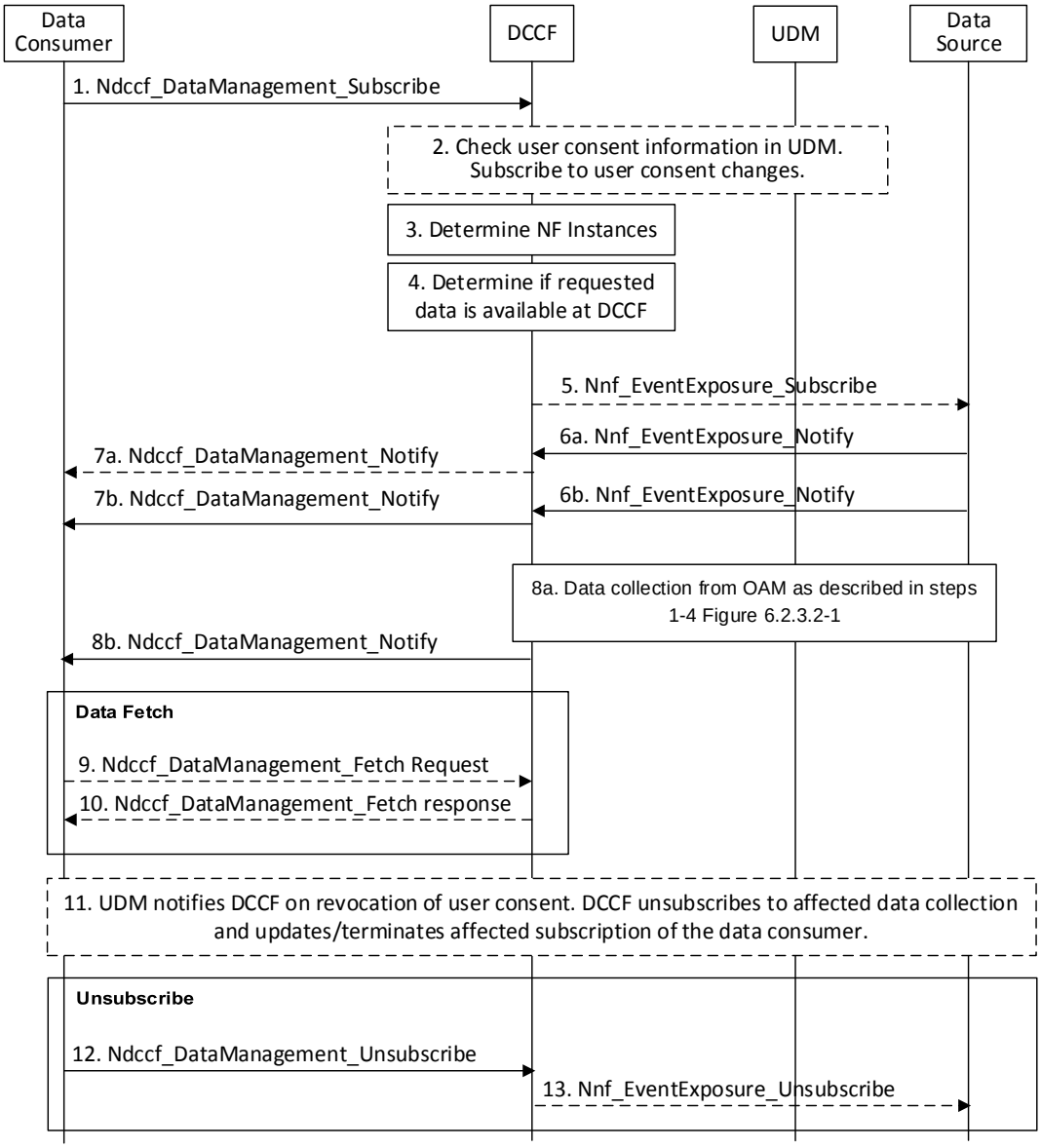

Figure 6.2.6.3.2-1: Data Collection via DCCF

1. The data consumer subscribes to data via the DCCF by invoking the Ndccf_DataManagement_Subscribe(Service_Operation, Data Specification, Formatting Instructions, Processing Instructions, NF (or NF-Set) ID, ADRF Information) service operation as specified in clause 8.2.2. The data consumer may specify one or more notification endpoints. If data to be collected is subject to user consent: if the data consumer checked user consent, the data consumer shall provide user consent check information (i.e. an indication that it has checked user consent), otherwise, the data consumer shall provide a purpose for the data collection.

   Service_Operation is the service operation to be used by the DCCF to request data (e.g. Namf_EventExposure_Subscribe or OAM Subscribe). Data Specification provides Service Operation-specific parameters (e.g. event IDs, UE-ID(s), target of event reporting) used to retrieve the data. Formatting and Processing Instructions are as defined in clause 5A.4. The data consumer may include the Data Source, e.g. NF Instance (or NF Set) ID from which the data needs to be collected. The data consumer may include ADRF information indicating whether the data are to be stored in an ADRF, and optionally an ADRF ID.

2. The DCCF checks if data is to be collected for a user, i.e. SUPI or GPSI, then, depending on local policy and regulations, the DCCF checks the user consent by retrieving the user consent information from UDM using Nudm_SDM_Get including data type "User consent" and taking into account purpose for data collection as provided in step 1. If user consent is not granted, DCCF does not subscribe to event exposure for events related

to this user, the data collection for this SUPI or GPSI stops here and DCCF sends a response to the data consumer indicating that user consent for data collection was not granted. If the user consent is granted, the DCCF subscribes to UDM to notifications of changes on subscription data type "User consent" for this user using Nudm_SDM_Subscribe.

If the data consumer is NWDAF and it provides user consent check information (i.e. an indication that it has checked user consent) in Ndccf_DataManagement_Subscribe in step 1, which has been obtained by the NWDAF from UDM before, then the DCCF can do data collection for a user based on the user consent information from the NWDAF and skip retrieving it from UDM.

3. The DCCF determine the NF type(s) and/or OAM to retrieve the data based on the Service Operation requested in step 1. If the NF instance or NF Set ID is not provided by the data consumer. the DCCF determines the NF instances that can provide data as described in clause 5A.2 and clause 6.2.2.2. If the consumer requested storage of data in an ADRF but the ADRF ID is not provided by the data consumer, or the collected data is to be stored in an ADRF according to configuration on the DCCF, the DCCF selects an ADRF to store the collected data.

4. The DCCF determines whether the data requested in step 1 are already being collected, as described in clause 5A.2.

   If the data requested are already being collected by a data consumer, the DCCF adds the data consumer to the list of data consumers that are subscribed for these data.

5. If the data subscribed in step 1 partially matches data that are already being collected by the DCCF from a Data Source, and a modification of this subscription to the Data Source would satisfy both the existing data subscriptions as well as the newly requested data, the DCCF invokes Nnf_EventExposure_Subscribe(Subscription Correlation ID) with parameters indicating how to modify the previous subscription (as specified in clause 5A.2). The DCCF adds the data consumer to the list of data consumers that are subscribed for these data.

   If the data requested at step 1 are not already available or not being collected yet, the DCCF subscribes to data from the NF using the Nnf_EventExposure_Subscribe service operation as specified in clause 5A.2 and clause 6.2.2.2, with DCCF indicated as Notification Target Address. The DCCF adds the data consumer to the list of data consumers that are subscribed for these data.

6. When new output data are available, the Data Source uses Nnf_EventExposure_Notify to send the data to the DCCF.

7. The DCCF uses Ndccf_DataManagement_Notify to send the data to all notification endpoints indicated in step 1. Data sent to notification endpoints may be processed and formatted by the DCCF so they conform to delivery requirements for each data consumer or notification endpoint as specified in clause 5A.4. The DCCF may store the information in ADRF if requested by the consumer or if required by DCCF configuration, using procedure as specified in clause 6.2B.3.

NOTE: According to Formatting Instructions provided by the data consumer, multiple notifications from a Data Source can be combined in a single Ndccf_DataManagement_Notify so many notifications from the Data Source result in fewer notifications (or one notification) to the data consumer. Alternatively, a notification can instruct the data notification endpoint to fetch the data from the DCCF before an expiry time.

8a. If DCCF needs to retrieve data from OAM, procedure for data collection from OAM as per steps 1-4 from clause 6.2.3.2 is used.

8b. The DCCF uses Ndccf_DataManagement_Notify to send the data to all notification endpoints indicated in step 1. Data sent to notification endpoints may be processed and formatted by the DCCF, so they conform to delivery requirements for each data consumer or notification endpoint as specified in clause 5A.4. The DCCF may store the information in ADRF if requested by the consumer or if required by DCCF configuration, using procedure as specified in clause 6.2B.3.

9. If a Ndccf_DataManagement_Notify contains a fetch instruction, the notification endpoint sends a Ndccf_DataManagement_Fetch request to fetch the data from the DCCF.

10. The DCCF delivers the data to the notification endpoint

11. The UDM may notify the DCCF on changes of user consent at any time after step 2. If user consent is no longer granted for a user for which data has been collected and there are no other consumers for the data, the DCCF shall unsubscribe to any Event ID to collect data for that SUPI or GPSI. The DCCF shall further update or

terminate affected subscriptions of the Data Consumer. The DCCF may unsubscribe to be notified of user consent updates from UDM for each SUPI for which user consent has been revoked.

12. When the data consumer no longer wants data to be collected it invokes Ndccf_DataManagement_Unsubscribe(Subscription Correlation ID), using the Subscription Correlation Id received in response to its subscription in step 1. The DCCF removes the data consumer from the list of data consumers that are subscribed for these data.

13. If there are no other data consumers subscribed to the data, the DCCF unsubscribes with the Data Source.

6.2.6.3.3 Historical Data Collection via DCCF

The procedure depicted in figure 6.2.6.3.3-1 is used by data consumers (e.g. NWDAF) to obtain historical data, i.e. data related to past time period. The data consumer requests data using Ndccf_DataManagement_Subscribe service operation. Whether the data consumer uses this procedure or directly contacts the ADRF or NWDAF is based on configuration.

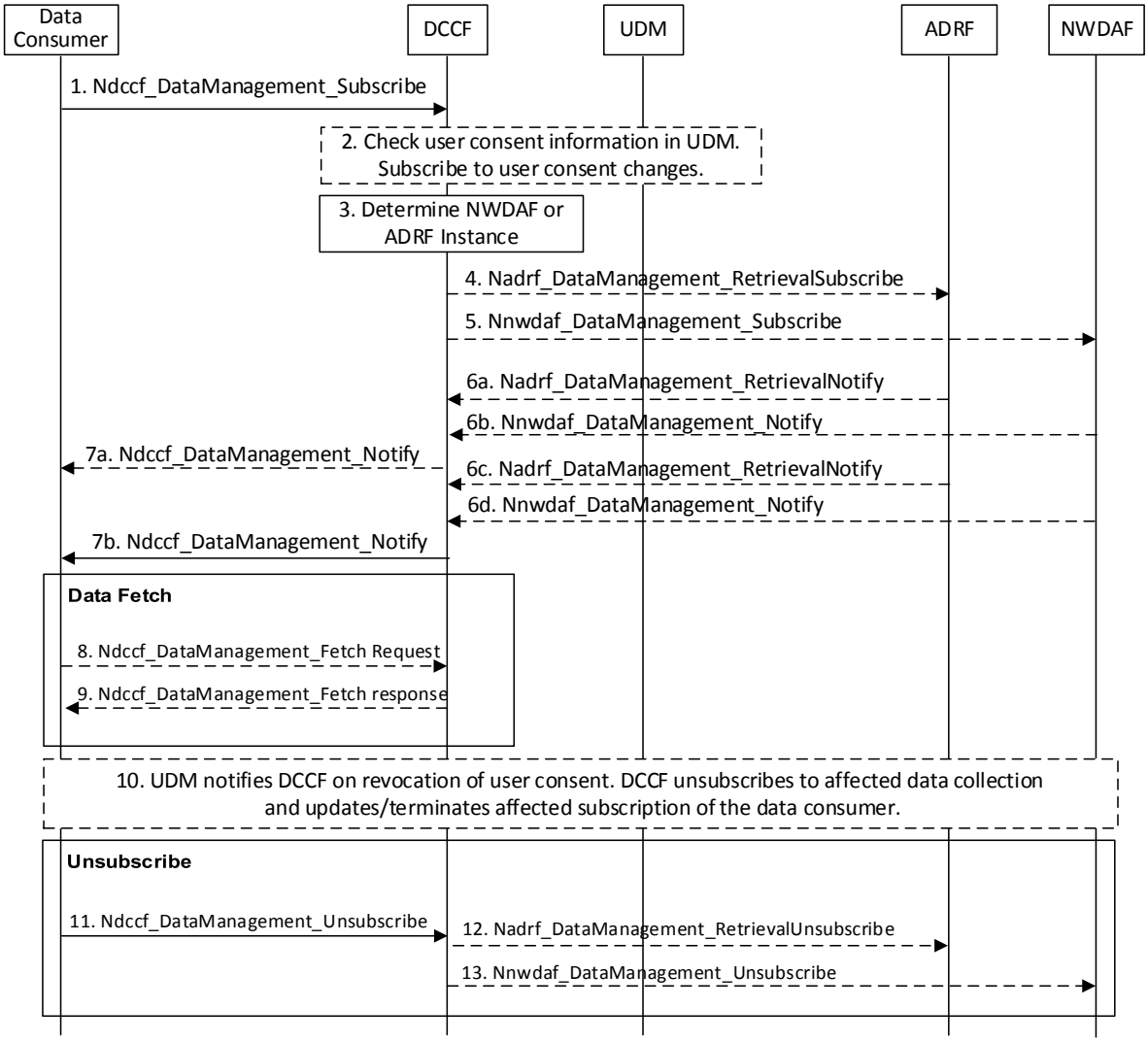

Figure 6.2.6.3.3-1: Historical Data Collection via DCCF

1. The data consumer requests data via DCCF by invoking the Ndccf_DataManagement_Subscribe(Service_Operation, Data Specification, Time Window, Formatting Instructions, Processing Instructions, ADRF ID or NWDAF ID (or ADRF Set ID or NWDAF Set ID) service operation as specified in clause 8.2.2. The data consumer may specify one or more notification endpoints to receive the data. If data to be collected is subject to user consent: if the data consumer checked user consent, the

data consumer shall provide user consent check information (i.e. an indication that it has checked user consent), otherwise, the data consumer shall provide a purpose for the data collection.

"Service_Operation" is the service operation used to acquire the data from a data source. "Data Specification" provides Service_Operation-specific parameters (e.g. event IDs, UE-ID(s)) used to retrieve the data. "Time Window" specifies a past time period and comprises a start and stop time. "Formatting and Processing Instructions" are as defined in clause 5A4. The data consumer may optionally include the ADRF or NWDAF instance (or ADRF Set or NWDAF Set) ID where the stored data resides.

2. The DCCF checks if data is to be collected for a user, i.e. SUPI or GPSI, then, depending on local policy and regulations, the DCCF checks the user consent by retrieving the user consent information from UDM using Nudm_SDM_Get including data type "User consent" and taking into account purpose for data collection as provided in step 1. If user consent is not granted, DCCF does not subscribe to event exposure for events related to this user, the data collection for this SUPI or GPSI stops here and DCCF sends a response to the data consumer indicating that user consent for data collection was not granted. If the user consent is granted, the DCCF subscribes to UDM to notifications of changes on subscription data type "User consent" for this user using Nudm_SDM_Subscribe.

   If the data consumer is NWDAF and it provides user consent check information (i.e. an indication that it has checked user consent) in Ndccf_DataManagement_Subscribe in step 1, which has been obtained by the NWDAF from UDM before, then the DCCF can do data collection for a user based on the user consent information from the NWDAF and skip retrieving it from UDM.

3. If an ADRF or NWDAF instance or ADRF Set ID or NWDAF Set ID is not provided by the data consumer, the DCCF determines if any ADRF or NWDAF instances might provide the data as described in clause 5B and 5A.2.

NOTE 1: An ADRF or NWDAF might have previously registered data it is collecting with the DCCF.

4. (conditional) If the DCCF determines that an ADRF instance might provide the data, or an ADRF instance or Set was supplied by the data consumer, the DCCF sends a request to the ADRF, using Nadrf_DataManagement_RetrievalSubscribe(Data Specification, Notification Target Address=DCCF) service operation as specified in clause 10.2. The ADRF responds to the DCCF with an Nadrf_DataManagement_RetrievalSubscribe response indicating if the ADRF can supply the data. If the data can be provided, the procedure continues with step 5.

5. (conditional) If the DCCF determines that an NWDAF instance might provide the data or an NWDAF instance or Set was supplied by the data consumer, the DCCF sends a request to the NWDAF using Nnwdaf_DataManagement_Subscribe(Data Specification, Notification Target Address=DCCF) as specified in clause 7.4.2.

6. The ADRF or the NWDAF sends the requested data (e.g. one or more stored notifications archived from a data source) to the DCCF. The data may be sent in one or more notification messages.

7. The DCCF uses Ndccf_DataManagement_Notify to send data to all notification endpoints indicated in step 1. Notifications are sent to the Notification Target Address(es) using the data consumer Notification Correlation ID(s) received in step 1. Data sent to notification endpoints may be processed and formatted by the DCCF, so they conform to delivery requirements specified by the data consumer.

NOTE 2: According to Formatting Instructions provided by the data consumer, multiple notifications from an ADRF or NWDAF can be combined in a single Ndccf_DataManagement_Notify so many notifications from the ADRF or NWDAF results in fewer notifications (or one notification) to the data consumer. Alternatively, a Ndccf_DataManagement_Notify can instruct the data notification endpoint to fetch the data from the DCCF before an expiry time.

8. If a notification contains a fetch instruction, the notification endpoint sends a Ndccf_DataManagement_Fetch request to fetch the data from the DCCF.

9. The DCCF delivers the data to the notification endpoint.

10. The UDM may notify the DCCF on changes of user consent at any time after step 2. If user consent is no longer granted for a user for which data has been collected and if there are no other consumers for the data, the DCCF shall unsubscribe to any data collection for that SUPI or GPSI. The DCCF shall further update or terminate

affected subscriptions of the Data Consumer. The DCCF may unsubscribe to be notified of user consent updates from UDM for each SUPI for which user consent has been revoked.

11. When the data consumer no longer wants data to be collected or has received all the data it needs, it invokes Ndccf_DataManagement_Unsubscribe(Subscription Correlation ID) as specified in clause 8.2.3, using the Subscription Correlation Id received in response to its subscription in step 1.

12. If the data are being provided by an ADRF and there are no other data consumers subscribed to the data, the DCCF unsubscribes with the ADRF using Nadrf_DataManagement_RetrievalUnsubscribe as specified in clause 10.2.7.

13. If the data are being provided by an NWDAF and there are no other data consumers subscribed to the data, the DCCF unsubscribes with the NWDAF using Nnwdaf_DataManagement_Unsubscribe as specified in clause 7.4.3.

6.2.6.3.4 Data Collection via Messaging Framework

This procedure depicted in Figure 6.2.6.3.4-1 is used by a data consumer (e.g. NWDAF) to obtain data and be notified of events using the DCCF and a Messaging Framework. The 3GPP DCCF Adaptor (3da) Data Management service and 3GPP Consumer Adaptor (3ca) Data Management service of the Messaging Framework Adaptor Function (MFAF) are used to interact with the 3GPP Network and the Messaging Framework. Whether the data consumer directly contacts the Data Source or goes via the DCCF is based on configuration.

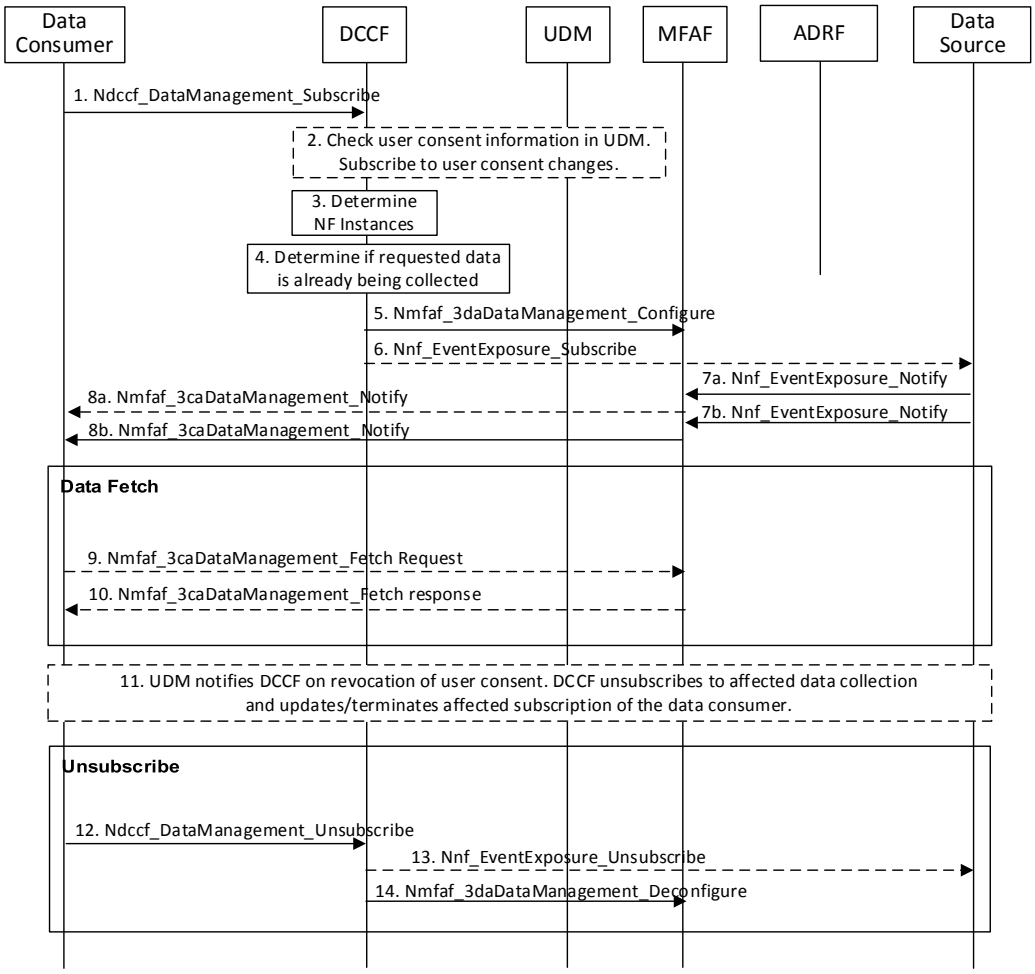

Figure 6.2.6.3.4-1: Data Collection via Messaging Framework

1. The data consumer subscribes to data via the DCCF by invoking the Ndccf_DataManagement_Subscribe(Service_Operation, Data Specification, Formatting Instructions, Processing

Instructions, NF (or NF-Set) ID, ADRF Information, Data Consumer Notification Target Address (+ Notification Correlation ID)) service operation as specified in clause 8.2.2. The data consumer may specify one or more notification endpoints and the NF or NF set to collect data from. If data to be collected is subject to user consent: if the data consumer checked user consent, the data consumer shall provide user consent check information (i.e. an indication that it has checked user consent), otherwise, the data consumer shall provide a purpose for the data collection.

Service_Operation is the service operation to be used by the DCCF to request data (e.g. Namf_EventExposure_Subscribe or OAM Subscribe). Data Specification provides Service_Operation-specific required parameters (e.g. event IDs, UE-ID(s), target of event reporting) and optional input parameters used to retrieve the data. Formatting and Processing Instructions are as defined in clause 5A.4. The data consumer may optionally include the Data Source NF Instance (or NF Set) ID. The data consumer may include ADRF information indicating whether the data are to be stored in an ADRF and, optionally, an ADRF ID.

NOTE 1: Data consumer requesting data to be stored in ADRF allows the collected data to be available to other data consumers in the future.

2. The DCCF checks if data is to be collected for a user, i.e. SUPI or GPSI, then, depending on local policy and regulations, the NWDAF checks the user consent by retrieving the user consent information from UDM using Nudm_SDM_Get including data type "User consent" and taking into account purpose for data collection as provided in step 1. If user consent is not granted, NWDAF does not subscribe to event exposure for events related to this user, the data collection for this SUPI or GPSI stops here and DCCF sends a response to the data consumer indicating that user consent for data collection was not granted. If the user consent is granted, the DCCF subscribes to UDM to notifications of changes on subscription data type "User consent" for this user using Nudm_SDM_Subscribe.

   If the data consumer is NWDAF and it provides user consent check information (i.e. an indication that it has checked user consent) in Ndccf_DataManagement_Subscribe in step 1, which has been obtained by the NWDAF from UDM before, then the DCCF can do data collection for a user based on the user consent information from the NWDAF and skip retrieving it from UDM.

3. If the NF instance or NF Set ID is not provided by the data consumer, the DCCF determines the NF instances that can provide data as described in clause 5A.2 and clause 6.2.2.2. If the consumer requested storage of data in an ADRF, but the ADRF ID is not provided by the data consumer, or the collected data is to be stored in an ADRF according to configuration on the DCCF, the DCCF selects an ADRF to store the collected data.

4. The DCCF determines whether the data requested in step 1 are already being collected, as described in clause 5A.2.

   If the data requested are already being collected by a data consumer, the DCCF adds the data consumer to the list of data consumers that are subscribed for these data.

5. The DCCF sends an Nmfaf_3daDataManagement_Configure(Data Consumer Information, MFAF Notification Information, Formatting Conditions, Processing Instructions) to configure the MFAF to map notifications received from the Data Source to outgoing notifications sent to endpoints, and to instruct the MFAF how to format and process the outgoing notifications. The DCCF may also instruct the MFAF to store data into ADRF by providing an ADRF ID, if requested by the data consumer in step 1, together with the NF Id of the data source.

   Data Consumer Information contains for each notification endpoint, the data consumer Notification Target Address (+ Data Consumer Notification Correlation ID to be used by the MFAF when sending notifications in step 9.

   MFAF Notification Information is included if a Data Source is already sending the data to the MFAF. MFAF Notification Information identifies Event Notifications received from the Data Sources and comprises the MFAF Notification Target Address (+ MFAF Notification Correlation ID). If the MFAF does not receive MFAF Notification information from the DCCF, the MFAF selects a MFAF Notification Target Address (+ MFAF Notification Correlation ID) and sends the MFAF Notification Information, containing MFAF Notification Target Address (+ MFAF Notification Correlation ID), to the DCCF in the Nmfaf_3daDataManagement_Configure Response.

6. If the data subscribed in step 1 partially matches data that are already being collected by the DCCF from a Data Source, and a modification of this subscription to the Data Source would satisfy both the existing data subscriptions as well as the newly requested data, the DCCF invokes

Nnf_EventExposure_Subscribe(Subscription Correlation ID) with parameters indicating how to modify the previous subscription (as specified in clause 5A.2). The DCCF adds the data consumer to the list of data consumers that are subscribed for these data.

If the data requested at step 1 are not already available or not being collected yet, the DCCF subscribes to data from the NF using the Nnf_EventExposure_Subscribe(Data Specification, MFAF Notification Target Address (+ MFAF Notification Correlation ID)) service operation as specified in clause 5A.2 and clause 6.2.2.2, using the MFAF Notification Target Address (+ MFAF Notification Correlation ID) received in step 5. The DCCF adds the data consumer to the list of data consumers that are subscribed for these data.

7. When new output data are available, the Data Source uses Nnf_EventExposure_Notify to send the data to the MFAF. The Notification includes the MFAF Notification Correlation ID.

8. The MFAF uses Nmfaf_3caDataManagement_Notify to send the data to all notification endpoints indicated in step 6. Notifications are sent to the Notification Target Address(es) using the Data Consumer Notification Correlation ID(s) received in step 6. Data sent to notification endpoints may be processed and formatted by the MFAF, so they conform to delivery requirements specified by the data consumer. The MFAF may store the information in ADRF if requested by consumer or if required by DCCF configuration

NOTE 2: According to Formatting Instructions provided by the data consumer, multiple notifications from a Data Source can be combined in a single Nmfaf_3caDataManagement_Notify, so many notifications from the Data Source results in fewer notifications (or one notification) to the data consumer. Alternatively, a notification can instruct the data notification endpoint to fetch the data from the MFAF before an expiry time.

9. If a Nmfaf_3caDataManagement_Notify contains a fetch instruction, the notification endpoint sends a Nmfaf_3caDataManagement_Fetch request to fetch the data from the MFAF.

10. The MFAF delivers the data to the notification endpoint.

11. The UDM may notify the DCCF on changes of user consent at any time after step 2. If user consent is no longer granted for a user for which data has been collected and if there are no other consumers for the data, the DCCF shall unsubscribe to any Event ID to collect data for that SUPI or GPSI. The DCCF shall further update or terminate affected subscriptions of the Data Consumer. The DCCF may unsubscribe to be notified of user consent updates from UDM for each SUPI for which user consent has been revoked.

12. When the data consumer no longer wants data to be collected, it invokes Ndccf_DataManagement_Unsubscribe(Subscription Correlation ID), using the Subscription Correlation Id received in response to its subscription in step 1. The DCCF removes the data consumer from the list of data consumers that are subscribed for these data.

13. If there are no other data consumers subscribed to the data, the DCCF unsubscribes with the Data Source.

14. The DCCF de-configures the MFAF so it no longer maps notifications received from the Data Source to the notification endpoints configured in step 5.

6.2.6.3.5 Historical Data Collection via Messaging Framework

The procedure depicted in figure 6.2.6.3.5-1 is used by data consumers (e.g. NWDAF) to obtain historical data, i.e. data related to past time period. The data consumer obtains data using Ndccf_DataManagement_Subscribe service operation as specified in clause 8.2.2, where the subscription results in one or more notifications depending on how the data is retrieved from the ADRF or NWDAF and how the data is formatted. Whether the data consumer uses this procedure or directly contacts the ADRF or NWDAF is based on configuration.

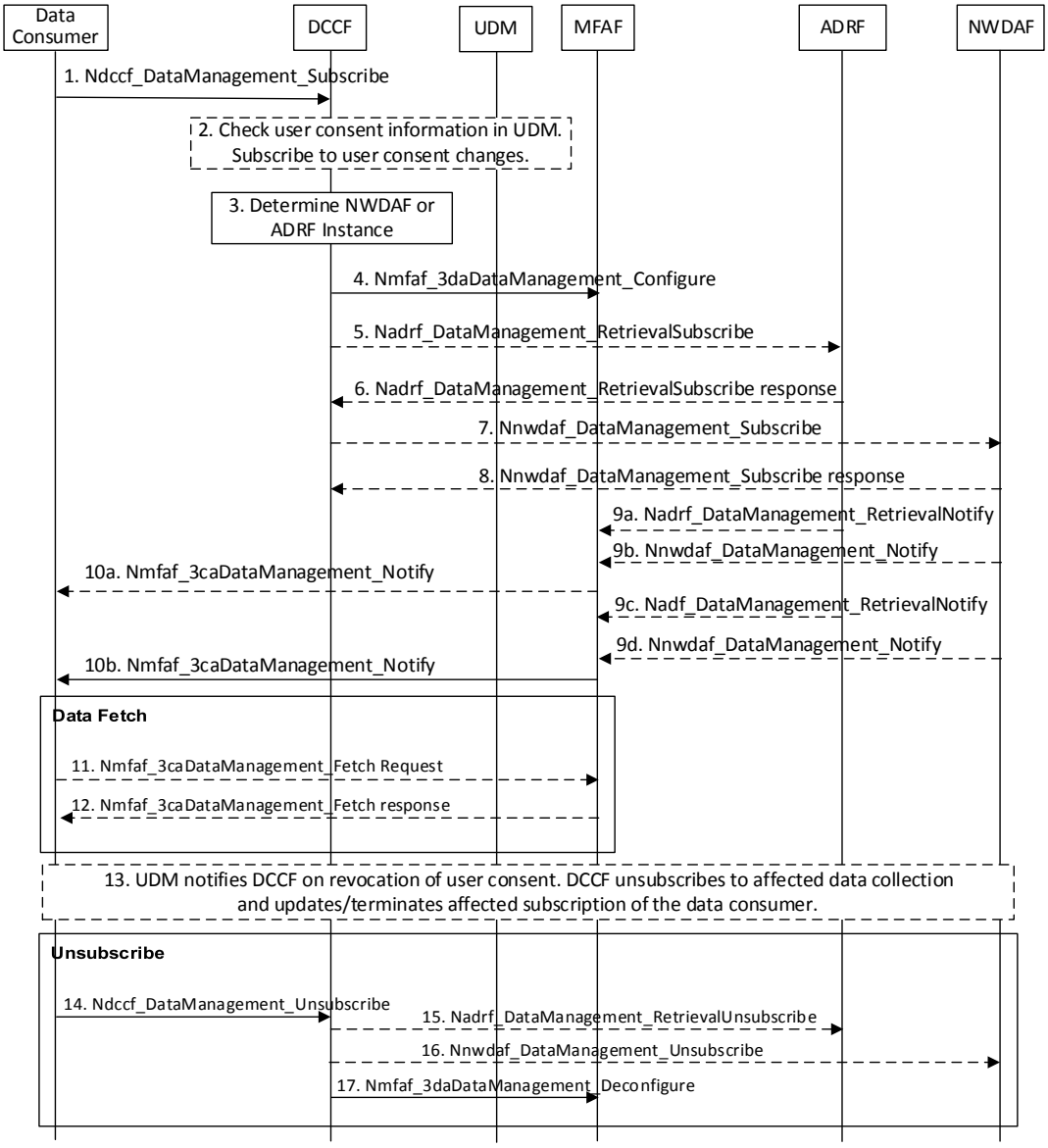

Figure 6.2.6.3.5-1: Historical Data Collection via Messaging Framework

1. The data consumer requests data via DCCF by invoking the Ndccf_DataManagement_Subscribe(Service Operation, Data Specification, Time Window, Formatting Instructions, Processing Instructions, ADRF ID or NWDAF ID (or ADRF Set ID or NWDAF Set ID) service operation as specified in clause 8.2.2. The data consumer may specify one or more notification endpoints to receive the data. If data to be collected is subject to user consent: if the data consumer checked user consent, the data consumer shall provide user consent check information (i.e. an indication that it has checked user consent), otherwise, the data consumer shall provide a purpose for the data collection.

   Service_Operation is the service operation used to acquire the data from a data source, Data Specification provides Service_Operation-specific required parameters (e.g. event IDs, UE-ID(s) and optional input parameters used to retrieve the data. Time Window specifies a past time period and comprises a start and stop time, and Formatting and Processing Instructions are as defined in clause 5A4. The data consumer may optionally include the ADRF or NWDAF instance (or ADRF Set or NWDAF Set) ID where the stored data resides.

2. The DCCF checks if data is to be collected for a user, i.e. SUPI or GPSI, then, depending on local policy and regulations, the DCCF checks the user consent by retrieving the user consent information from UDM using Nudm_SDM_Get including data type "User consent" and taking into account purpose for data collection as provided in step 1. If user consent is not granted, DCCF does not subscribe to event exposure for events related

to this user, the data collection for this SUPI or GPSI stops here and DCCF sends a response to the data consumer indicating that user consent for data collection was not granted. If the user consent is granted, the DCCF subscribes to UDM to notifications of changes on subscription data type "User consent" for this user using Nudm_SDM_Subscribe.

If the data consumer is NWDAF and it provides user consent check information (i.e. an indication that it has checked user consent) in Ndccf_DataManagement_Subscribe in step 1, which has been obtained by the NWDAF from UDM before, then the DCCF can do data collection for a user based on the user consent information from the NWDAF and skip retrieving it from UDM.

3. If an ADRF or NWDAF instance or ADRF Set ID or NWDAF Set ID is not provided by the data consumer, the DCCF determines if any ADRF or NWDAF instances might provide the data as described in clause 5B and 5A.2.

NOTE 1: An ADRF or NWDAF might have previously registered data it is collecting with the DCCF.

4. The DCCF sends an Nmfaf_3daDataManagement_Configure(Data Consumer Information, Formatting Conditions, Processing Instructions) to configure the MFAF to map notifications received from the ADRF or NWDAF to outgoing notifications sent to endpoints, and to instruct the MFAF how to format and process the outgoing notifications.

   "Data Consumer Information" contains for each notification endpoint, the data consumer Notification Target Address (+ Data Consumer Notification Correlation ID) to be used by the MFAF when sending notifications. The MFAF selects an MFAF Notification Target Address (+ MFAF Notification Correlation ID) and sends the MFAF Notification Information, containing MFAF Notification Target Address (+ MFAF Notification Correlation ID), to the DCCF in the Nmfaf_3daDataManagement_Configure Response.

5. (conditional) If the DCCF determines that an ADRF instance might provide the data, or an ADRF instance or Set was supplied by the data consumer, the DCCF sends a request to the ADRF, using Nadrf_DataManagement_RetrievalSubscribe(Data Specification, MFAF Notification Information) containing the MFAF Notification Target Address (+ MFAF Notification Correlation ID) received in step 4 as specified in clause 10.2.

6. The ADRF responds to the DCCF with an Nadrf_DataManagement_RetrievalSubscribe response indicating if the ADRF can supply the data. If the data can be provided, the procedure continues with step 9.

7. (conditional) If the DCCF determines that an NWDAF instance might provide the data, or an NWDAF instance or NWDAF Set was supplied by the data consumer, the DCCF sends a request to the NWDAF, using Nnwdaf_DataManagement_Subscribe(Data Specification, MFAF Notification Information) as specified in clause 7.4.2. MFAF Notification Information contains the MFAF Notification Target Address (+ MFAF Notification Correlation ID) received in step 4.

8. The NWDAF responds to the DCCF with an Nnwdaf_DataManagement_Subscribe response indicating if the NWDAF can supply the data.

9. The ADRF uses Nadrf_DataManagement_RetrievalNotify or the NWDAF uses Nnwdaf_DataManagement_Notify to send the requested data (e.g. one or more stored notifications archived from a data source) to the MFAF. The data may be sent in one or more notification messages.

10. The MFAF uses Nmfaf_3caDataManagement_Notify to send data to all notification endpoints indicated in step 4. Notifications are sent to the Notification Target Address(es) using the Data Consumer Notification Correlation ID(s) received in step 4. Data sent to notification endpoints may be processed and formatted by the MFAF, so they conform to delivery requirements specified by the data consumer.

NOTE 2: According to Formatting Instructions provided by the data consumer, multiple notifications from an ADRF or NWDAF can be combined in a single Nmfaf_3caDataManagement_Notify so many notifications from the ADRF or NWDAF results in fewer notifications (or one notification) to the data consumer. Alternatively, a Nmfaf_3caDataManagement_Notify can instruct the data notification endpoint to fetch the data from the MFAF before an expiry time.

11. If a notification contains a fetch instruction, the notification endpoint sends a Nmfaf_3caDataManagement_Fetch request as specified in clause 9.3.3 to fetch the data from the MFAF.

12. The MFAF delivers the data to the notification endpoint.

13. The UDM may notify the DCCF on changes of user consent at any time after step 2. If user consent is no longer granted for a user for which data has been collected and if there are no other consumers for the data, the DCCF shall unsubscribe to any data collection for that SUPI or GPSI. The DCCF shall further update or terminate affected subscriptions of the Data Consumer. The DCCF may unsubscribe to be notified of user consent updates from UDM for each SUPI for which user consent has been revoked.

14. When the data consumer no longer wants data to be collected or has received all the data it needs, it invokes Ndccf_DataManagement_Unsubscribe(Subscription Correlation ID), using the Subscription Correlation Id received in response to its subscription in step 1.

15. If the data are being provided by an ADRF and there are no other data consumers subscribed to the data, the DCCF unsubscribes with the ADRF using Nadrf_DataManagement_RetrievalUnsubscribe as specified in clause 10.2.7.

16. If the data are being provided by an NWDAF and there are no other data consumers subscribed to the data, the DCCF unsubscribes with the NWDAF using Nnwdaf_DataManagement_Unsubscribe as specified in clause 7.4.3.

17. The DCCF de-configures the MFAF so it no longer maps notifications received from the ADRF or NWDAF to the notification endpoints configured in step 4.

6.2.6.3.6 Data collection profile registration

In some cases data consumers (e.g. NWDAF or ADRF) collect data from data source NF directly, e.g. when NWDAF is co-located with 5GC NF.

To enable data consumers can get the data which has been collected by NWDAF or ADRF directly (i.e. not via DCCF), the NWDAF or ADRF may register/update the data collection profile to the DCCF during/after the procedure of data collection. DCCF can then determine some requested data is available in NWDAF or ARDF and can coordinate data collection based on the data collection profile.

The procedure depicted in Figure 6.2.6.3.6-1 is used by data source(e.g. NWDAF or ADRF) to register data profile to DCCF.

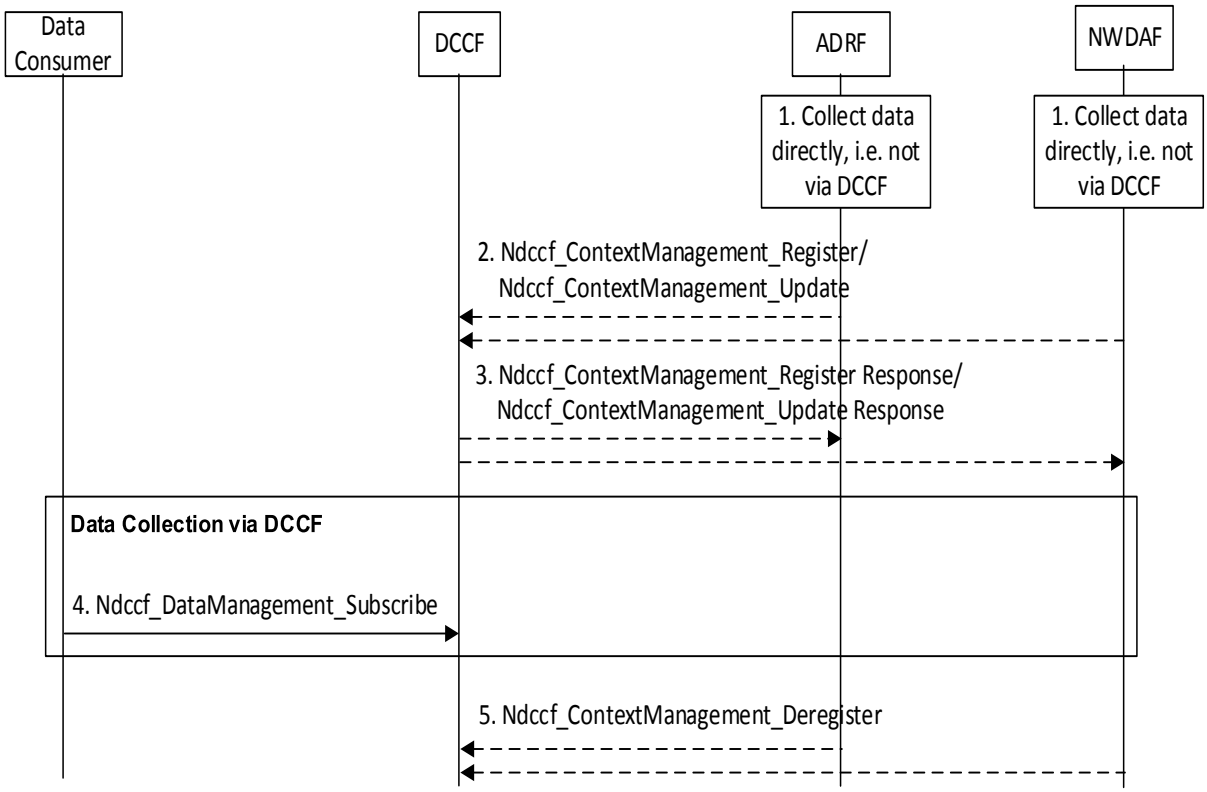

Figure 6.2.6.3.6-1: Procedure for the NWDAF or ADRF register data profile to DCCF

1. An ADRF or NWDAF instance is collecting or has collected data directly, e.g. from collocated NF.

2. The ADRF or NWDAF requests to register/update data collection profile (Service Operation, Analytics/Data Specification, ADRF ID or NWDAF ID) to DCCF by invoking the Ndccf_ContextManagement_Register or Ndccf_ContextManagement_Update. The registration/ update request can be triggered by the acceptation of subscription for data collection responded by the data source (e.g. collocated NF), it can be before the start of data collection or after the completion of data collection. DCCF determines the data collection status of NWDAF or ADRF based on the Analytics/Data Specification, i.e. DCCF determines whether the required data is being collected or has been collected.

   "Service Operation" identifies the service used to collect the data or analytics from a Data Source (e.g.: Namf_EventExposure_Subscribe or Nnwdaf_AnalyticsSubscription_Subscribe).

   "Analytics/Data Specification" is the "Service Operation" specific parameters that identify the collected data (i.e.: Analytics ID(s) / Event ID (s), Target of Analytics Reporting or Target of Event Reporting, Analytics Filter or Event Filter, etc.).

   NWDAF ID or ADRF ID specify the ADRF or NWDAF which registers data collection profile.

3. The DCCF responds to the ADRF or NWDAF with a Ndccf_ContextManagement_Register Response or Ndccf_ContextManagement_Update Response.

4. To obtain historical data and if the data consumer is configured to be collect data via the DCCF using Ndccf_DataManagement_Subscribe service operation, the data consumer uses the procedures described in clause 6.2.6.3.2 or clause 6.2.6.3.3.

5. The ADRF or NWDAF requests to delete a registration of data collection or analytics collection to the DCCF by invoking the Ndccf_ContextManagement_Deregister.

6.2.7 Data Collection with Event Muting Mechanism

6.2.7.1 General

Additional mechanisms to limit signalling between Event Producer NF (e.g. AMF, SMF) and Event Consumer NF (NWDAF, DCCF) are provided, with the Event Provider NFs enhanced with the optional capability of muting the notification of the events while storing for a limited time and limited size the events until the Event Consumer NF retrieves such mute stored events.

6.2.7.2 Procedure for Data Collection with Event Muting Mechanism

The mute storage of events mechanism in the DCCF, the NWDAF, or NFs reuses the Event Reporting Information field of Event Exposure Framework to include the following flags:

- Deactivate notification flag: The event consumer NF includes in the subscription to an event ID the deactivation flag to indicate to the event provider NF to collect, store the requested events but halt the notification to the consumer. The number of stored events may be limited based on NF configuration; when this number is reached, the NF continues to store new events and deletes the oldest events.

- Retrieval notification flag: The event consumer NF includes in an event subscription modification request the subscription identification and the retrieval notification flag to indicate to the event producer NF to send the past collected events not already sent to this consumer NF. After sending the past collected events the event producer continues to store events without sending notifications to the event consumer.

Using the event muting mechanism NWDAF, DCCF can subscribe to events from NFs such as AMF and SMF, to avoid constant notifications and retrieve the mute stored events when it requires.

The procedure in Figure 6.2.7.2-1 is used by Event Consumer NF to control the frequency of data collection from Event Producer NFs (except DCCF and NWDAF) via Event Exposure. For data collection via DCCF and NWDAF, the consumer may mute the notifications by using the formatting instructions as specified in clause 5A.4 or the Bulked Data Formatting and Processing parameters as specified in clause 6.2.6.1.

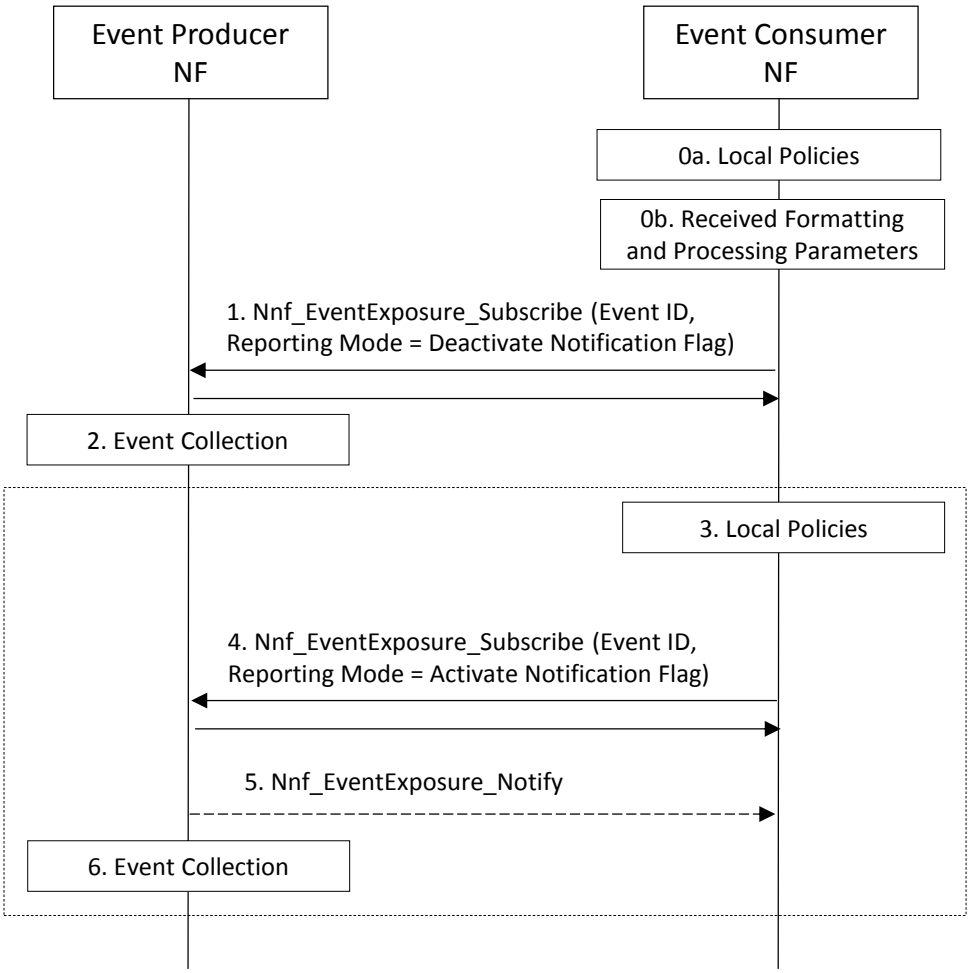

Figure 6.2.7.2-1: Procedure for muting event notification

0a. The Event Consumer NF, such as NWDAF or DCCF, is configured with local policies that are used to determine when the muted storage of events is triggered.

0b. The Event Consumer NF, such as NWDAF or DCCF, may receive a request with the Formatting and Processing parameters indicating Event Clubbing. The DCCF or NWDAF may utilize event muting when collecting data from NFs.

1. The Event Consumer NF, DCCF or NWDAF subscribes for a (set of) Event ID(s) by invoking the Nnf_EventExposure_Subscribe service operation including in event reporting information the deactivate notification flag.

   If the Event Producer NF supports the deactivate notification flag, the Event Producer NF sends a response back including the Subscription Correlation ID and an indication of successful deactivation of notifications. The Event Consumer NF may request the Event Producer NF to store data related to Event ID(s), or aggregated data related to UE(s).

   If the Event Producer NF does not support the deactivate notification flag, the Event Producer NF sends a response back including an indication of failure. In this case, the Event Consumer NF re-sends the subscription request without including in the event reporting information the deactivate notification flag.

NOTE: If the Event Producer NF receives a subscription without the deactivate notification flag, the steps 2 - 6 are not executed and the Event Producer NF performs the event notification as defined in TS 23.502 [3], clause 4.15

2. Based on the request from Event Consumer NF, DCCF or NWDAF, the Event Producer NF triggers a window of event collection for the Event Consumer NF, DCCF or NWDAF subscription with the indication of "deactivate notification flag". The Event Producer NF keeps the association between the Event ID, Subscription Correlation ID (which identifies the consumer of the event), subscriber information (e.g. notification target information) and

the status of the transaction between the Event Consumer NF, DCCF or NWDAF and the Event Producer as "collecting events / non-notification".

3. Based on local policies or based on the Notification Time Window indicated in the Formatting and Processing parameters of the received request in step 0b, the Event Consumer NF, DCCF or NWDAF decides when to request the muted stored events from the Event Producer NF.

4. Event Consumer NF invokes the Nnf_EventExposure_Subscribe service operation from the Event Producer NF including, the Event ID, the Subscription Correlation ID, and the retrieval notification flag. These parameters denote the identification of the transaction required by the Event Consumer NF, i.e. retrieve muted stored events for a subscribed Event ID and trigger a new time window of muted stored event generation without notification.

5. Event Producer NF based on the parameters received in the request from Event Consumer NF verifies whether there is a subscription to the requested Event ID with a deactivate notification flag. In positive case, Event Producer NF identifies and sends the past collected events muted during the period between the received retrieval notification flag and the last deactivate flag received from the Event consumer NF for the Event ID, the Subscription Correlation ID.

6. The Event Producer NF checks whether overall event reporting information (e.g. the maximum time window for the subscription of such Event ID) has expired. If yes, it does not trigger another round of event muted storage and deactivates the subscription. If not expired, the Event Producer NF trigger another time window for muted stored of produced events, sets back the deactivated notification flag for the Event ID and Subscription Correlation ID.

If the Event Consumer NF wants to change an existing subscription to an Event Producer NF using muted stored events into a regular notification of events, it shall invoke Nnf_EventExposure_Subscribe service operation from Event Producer NF without deactivate notification flag.

6.2.8 Data Collection from the UE Application

6.2.8.1 General

The NWDAF may interact with an AF to collect data from UE Application(s) as an input for analytics generation and ML model training. The AF can be in the MNO domain or an AF external to MNO domain. The data collection request from NWDAF may trigger the AF to collect data from the UE Application. The AF in this clause is referred as the Data Collection AF which is described in TS 26.531 [32].

The UE Application establishes a connection to the AF in the MNO domain or external to MNO domain over user plane via a PDU session. The AF communicates with the UE Application and collects data from UE Application.

For both an AF in trusted domain and an AF in untrusted domain (which supports to collect data from a UE Application), the SLA between the operator and the Application Service Provider (i.e. ASP) determines per Application ID in use by the ASP:

- The AF for the UE Application to connect to (e.g. based on an FQDN).
- The information that the UE Application shares with the AF, subject to user consent.
- Possible Data Anonymization, Aggregation or Normalization algorithms (if used).
- The authentication information that enable the AF to verify the authenticity of the UE's Application that provides data.

NOTE 1: The mutual authentication info that is used by the UE Application and the AF and how user consent is obtained is out of SA WG2's scope.

The AF (which supports the data collection) is configured based on the SLA above.

NOTE 2: Data Anonymization, Aggregation or Normalization algorithms within the SLA are defined per individual UE.

A UE Application (which supports to providing data to an AF) is configured by the ASP with the Application ID to use in the communication with the AF and then the UE Application is configured per Application ID with the following information:

- The address of the AF to contact.
- The parameters that the UE Application is authorized to provide to the AF.
- The authentication information to enable the UE Application to verify the authenticity of the AF that requests data.

NOTE 3: The authentication and authorization info that is used by the UE Application and the AF for collection and how user consent is obtained is out of SA2's scope.

NOTE 4: The configuration procedure for the above information from the ASP to the UE's Application is out of SA WG2 scope.

NOTE 5: The Application ID configured in the UE Application can either be an OSAppId as defined in TS 23.503 [4] or an OS independent Application Identifier (e.g. for applications running on a web browser).

The Target for Event Reporting in the Naf_EventExposure request may be set to:

- an external UE ID (i.e. GPSI) or an external Group ID, in case the AF is located in the untrusted domain;
- a SUPI or an internal Group ID, in case the AF is located within the trusted domain.

The GPSI may be an External Identifier for individual UE as defined in TS 23.501 [2] that includes the domain name. This domain name and the Application ID configured in the UE Application are different from each other.

6.2.8.2 Procedure for data collection from the UE Application

6.2.8.2.1 Connection establishment between UE Application and AF

The UE Application receives the data collection configuration from ASP. The configuration information is as described in clause 6.2.8.1.

The UE Application establishes a user plane connection to the AF. Data collection procedure from the UE Application is performed via the user plane connection.

NOTE 1: Whether multiple user plane connections are established, or a single user plane connection is established for different applications between each UE Application and AF is based on implementation that is out of 3GPP scope.

NOTE 2: The Connection establishment procedure from the UE Application to the AF as above is out of scope of the present specification. For the 3GPP defined services, the Connection establishment procedure is in the scope of SA WG4. For the non-3GPP defined services, the Connection establishment procedure is out of 3GPP's scope.

NOTE 3: In order to preserve resources (e.g. battery, quota) for the end user, a user plane connection to the AF can be established only when the UE has an active PDU Session for the UE Application and it is actively using the network (i.e. the user plane connection to the AF does not need to be established when the UE Application is inactive, or used in an off-line mode).

Both direct data collection procedure (from the UE Application to the AF, either in trusted domain or untrusted domain) and indirect data collection procedure (from the UE Application to the Application server and from the Application server to the AF) shall be supported. The data collection procedure is described in TS 26.531 [32].

The AF retrieves and stores the IP address of the UE (in the PDU session used) in order to request data collection from the UE Application. The UE IP address is used by the AF to identify the user plane connection.

NOTE 4: An operator can deploy NAT functionality in the network; Data collection from the UE Application when NAT is deployed is not specified in this release of the specification.

The UE Application provides the Application ID configured in the UE Application to the AF as described in TS 26.531 [32].

6.2.8.2.2 AF registration and discovery

The AF registers its available NF profile to the NRF. The AF in trusted domain registers to the NRF by using the Nnrf_NFManagement service that is defined in clause 5.2.7.2 of TS 23.502 [3]. The AF in untrusted domain registers the available NF profile to the NRF via the NEF as described in clause 6.2.2.3.

The AF discovery and selection is described in TS 23.502 [3].

6.2.8.2.3 Data Collection Procedure from UE

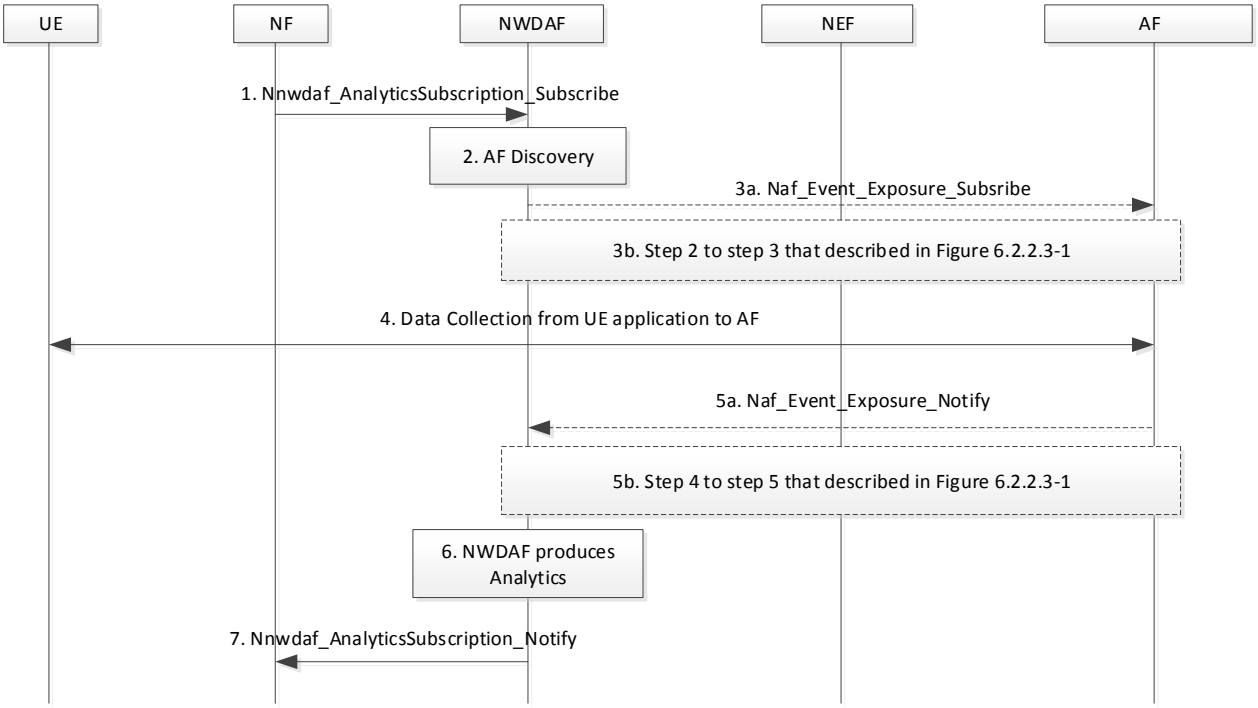

Figure 6.2.8.2.3-1: Data Collection Procedure from UE

1. An NF subscribes to analytics from the NWDAF as described in clause 6.1.1.1, that includes Analytics ID, Analytics Filter Information including e.g. AoI, Internal Application ID(s) and Target of Analytics Reporting. NWDAF may also initiate the data collection prior to this subscription.

NOTE: Subscription to analytics can be triggered directly towards NWDAF or can be done via DCCF using procedure in clause 6.1.4.2.

2. NWDAF discovers the AF that provides data collection (based on the AF profiles registered in NRF) as described inTS 23.502 [3].

Step 3a is used for the AF in trusted domain while step 3b is used for the AF in untrusted domain.

3a. NWDAF subscribes to the AF in trusted domain for UE data collection (i.e. input data from UE for analytics), by using Naf_EventExposure_Subscribe as defined in clause 5.2.19.2 of TS 23.502 [3]. The NWDAF request contains an Application ID known in the core network and the UE Application provides the Application ID configured in the UE Application. The AF binds the NWDAF request for an Application Id and the UE data collection for an Application Id configured in the UE.

3b. NWDAF subscribes to the AF in untrusted domain for UE data collection (i.e. input data from UE for analytics), by using step 2 and step 3 of the procedure that is described in Figure 6.2.2.3-1.

NOTE: For steps 3a and 3b, data collection can also be triggered using DCCF, as specified in clause 6.2.6.3.

4. The AF collects the UE data using either direct or indirect data collection procedure in clause 6.2.8.2.1. The establishment of the connection can be performed at any time prior to this. The AF links the data collection request from step 3 to the user plane connection as described in clause 6.2.8.2.4.

NOTE 1: The Direct data collection and indirect data collection procedure is described in TS 26.531 [32].

Step 5a is used for the AF in trusted domain while step 5b is used for the AF in untrusted domain.

5a. The AF in trusted domain receives the input data from the UE, and processes the data (e.g. anonymizes, aggregates and normalizes) according to the SLA that is configured in the AF described in clause 6.2.8.1 and Event ID(s) and Event Filter(s) set during step 3a. The trusted AF then notifies the NWDAF on the processed data according to the NWDAF subscription in step 3a.

5b. The AF in untrusted domain receives the input data from the UE, and processes the data (e.g. anonymizes, aggregates and normalizes) according to the SLA that is configured in the AF described in clause 6.2.8.1 and Event ID(s) and Event Filter(s) set during step 3b. The untrusted AF notifies the NWDAF on the processed data by using step 5b (i.e. Step 4 and step 5 of the procedure that described in Figure 6.2.2.3-1).

NOTE 2: If NWDAF requests the same data from multiple UEs, i.e. a determined list of UEs or "any UE" as the Target of Analytics Reporting, the AF can process (e.g. anonymize, aggregate and normalize) the data from multiple UEs according to the Event ID(s) and Event Filter(s) received from NWDAF during step 3a or 3b before notifying the NWDAF on the processed data in step 5a (if the AF is in trusted domain) or step 5b (if the AF is in untrusted domain).

6. The NWDAF produces analytics using the UE data received from the AF.

7. The NWDAF provides analytics to the consumer NF.

If the Target of Analytics Reporting that was received from the consumer in step 1 includes an Internal Group ID, NWDAF includes such Internal Group ID in step 3a or step 3b to AF. In the case of step 3b, NEF translates the Internal Group ID to an External Group ID.

If the Target of Analytics Reporting that was received from consumer in step 1 is "any UE", NWDAF may either set the target of event reporting to "any UE" in step 3a or 3b to AF, or may determine a list of SUPIs from AMF and/or SMF based on the Analytics Filter Information and sends the step 3a or 3b to AF for the determined list of UEs.

NOTE 3: It is assumed that the AF is provisioned with the list of UE IDs (GPSIs or SUPIs) belonging to an External or Internal Group ID.

6.2.8.2.4 Correlation between UE data collection and the NWDAF data request

6.2.8.2.4.1 General

The UE IP address is used to identify the user plane connection established between the UE application and the AF for data collection, while the AF receives the Naf_EventExposure_Subscribe to request for the specific UE data collection by using SUPI (for AF in trusted domain) or external UE ID (i.e. GPSI) (for AF in untrusted domain). AF is required to correlate the UE IP address to the SUPI or to GPSI.

If the AF supports requests addressed to External Group ID (for AF in untrusted domain) or Internal Group ID (for AF in internal trust domain), the AF must correlate the list of external UE ID (i.e. GPSI) or SUPI, respectively, with the group(s) the UE belongs to, so that the AF can further correlate the UE ID (external or internal) to the UE IP address.

AF may indicate in NF profile and register to NRF in clause 6.2.8.2.2 if it supports to do the mapping itself or ask NWDAF to do it. If the AF is in a trusted domain, it may also indicate the supported list of S-NSSAI, DNN combinations to NRF in NF profile.

Accordingly, if AF supports the mapping, for AF in trusted domain, it is required to correlate the UE IP address and SUPI as described in clause 6.2.8.2.4.2 after receiving the data collection request from NWDAF and there is no mapping information storage in the AF. For AF in untrusted domain, the procedure to correlate the UE IP address and GPSI is described in clause 6.2.8.2.4.4.

NWDAF may collect the mapping information as described in clause 6.2.8.2.4.4 before sending request to AF in step 3a or step 3b in Figure 6.2.8.2.3-1.

If the user plane session between the UE and the AF is released, the AF / NWDAF shall remove the stored correlation information between UE IP address / prefix and UE SUPI / GPSI.

For all procedures defined in this clause 6.2.8.2.4.3, a specific combination of S-NSSAI/DNN shall be corresponding to a single PDU session for a UE to access the AF (either in trusted domain or untrusted domain).

NOTE: Based on implementation, for the UE to access the Data Collection AF, only a single PDU Session is allowed to be established to the Data Collection AF, by configuring a specific S-NSSAI/DNN for the Data Collection AF only.

6.2.8.2.4.2 AF in trusted domain correlates UE data collection and NWDAF request

If the AF receives the Naf_EventExposure_Subscribe/Request including Target for Event Reporting set to SUPI and not including the UE's IP address and the AF does not locally store the UE's IP address, the AF finds the PDU session(s) serving the SUPI, DNN, S-NSSAI from UDM and the allocated IPv4 address or IPv6 prefix or both from SMF as described in Figure 6.2.8.2.4.2-1.

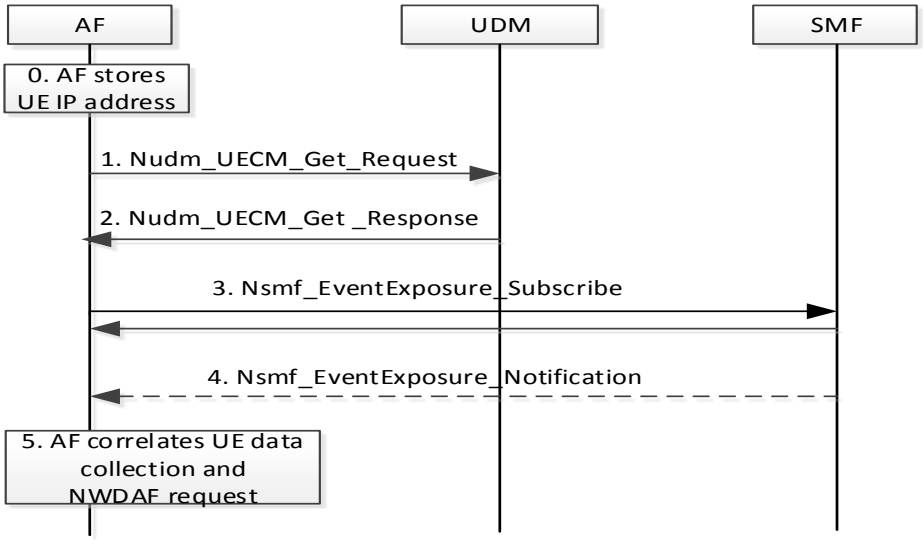

Figure 6.2.8.2.4.2-1: AF in trusted domain correlates UE data collection and NWDAF request

0. At the establishment of the user plane connection between the UE Application and the AF, the AF stores the UE IP address (for both direct and indirect reporting) as described clause 6.2.8.2.1.

1. The AF receives a request to retrieve input data as described in clause 6.2.8.2.3 including a SUPI. The AF finds the SMF serving the PDU session(s) for this SUPI using Nudm_UECM_Get_Request including SUPI, type of requested information set to SMF Registration Info and the S-NSSAI and DNN, as defined in clause 5.3.2.5.7 in TS 29.503 [26].

2. The UDM provides the SMF id and the corresponding PDU Session id, S-NSSAI, DNN using Nudm_UECM_Get_Response to the AF. Using the AF supported S-NSSAI, DNN and the received information from UDM, AF determines the PDU session used for the user plane connection between UE and AF.

3. The AF sends Nsmf_EventExposure_Subscribe to the SMF identified in step 2, including the Target for Event Reporting set to the PDU Session id(s) provided in step 2 and the Event ID set to IP address/prefix allocation/change.

4. The SMF provides the allocated IPv4 address or IPv6 prefix to the AF.

5. The AF correlates the UE data that includes the UE IP address and the NWDAF request for a SUPI using the retrieved IPv4 address or IP v6 prefix.

If the user plane session between the UE and the AF is released, the AF shall remove the stored correlation information between the UE IP address / prefix and SUPI.

6.2.8.2.4.3 AF in untrusted domain correlates UE data collection and NWDAF request

If the AF receives the Naf_EventExposure_Subscribe from NWDAF, via NEF, including Target for Event Reporting set to GPSI and not including the UE's IP address and the AF does not locally store the UE's IP address, the AF request the NEF to provide the allocated IPv4 address or IPv6 prefix or both as described in Figure 6.2.8.2.4.3-1.

NOTE 1: The NWDAF can also provide the UE IP address to the AF as described in clause 6.2.8.2.4.1.

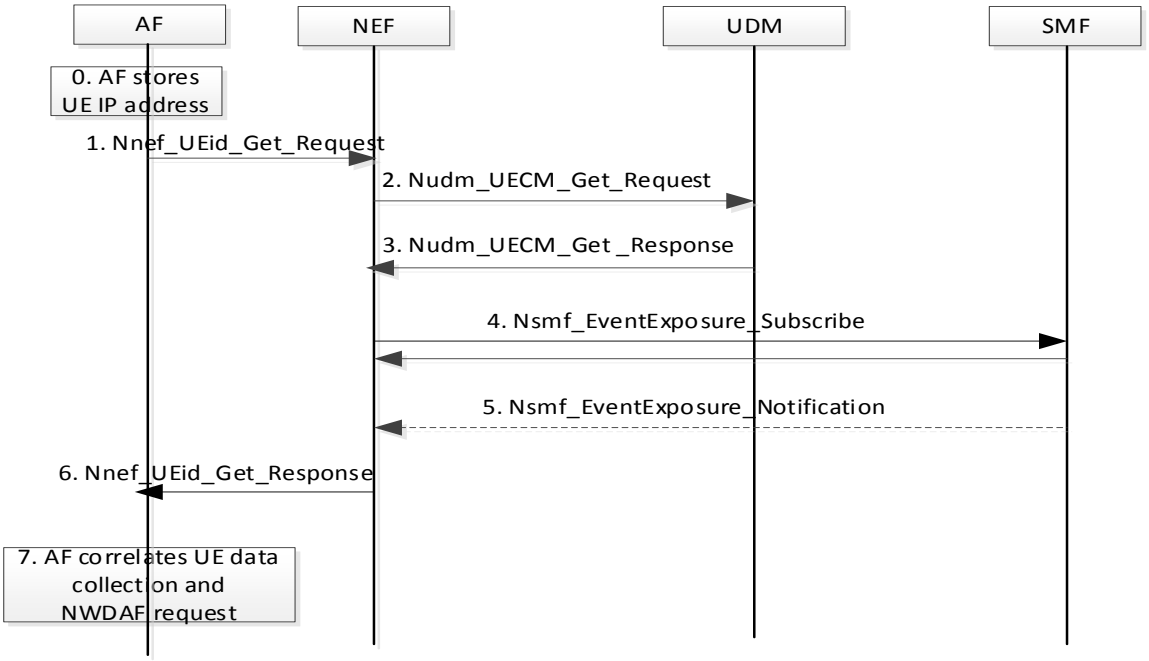

Figure 6.2.8.2.4.3-1: AF in untrusted domain correlates UE data collection and NWDAF request

0. Same step as step 0 in figure 6.2.8.2.4.3-1.

1. The AF receives a request to retrieve input data as described in clause 6.2.8.2.3 including a GPSI. The AF requests NEF to provide the IPv4address or IPv6 prefix or both serving the PDU session for this GPSI towards the AF using Nnef_UEid_Get_Request.

2. The NEF is configured with the DNN, S-NSSAI to access this AF. The NEF finds the SMF serving the PDU session(s) for this GPSI, DNN, S-NSSAI using Nudm_UECM_Get_Request including type of requested information set to SMF Registration Info and the S-NSSAI and DNN, as defined in clause 5.3.2.5.7 of TS 29.503 [26].

NOTE 2: If there are more than one (DNN, S-NSSAI) combination to access this AF, the NEF will find the SMF(s) serving the PDU session(s) to any of these (DNN, S-NSSAI) combinations.

3. The UDM provides the SMF id(s) and the tuple (PDU Session id (S-NSSAI, DNN) using Nudm_UECM_Get_Response to the NEF. Using the configuration in NEF, as described in step 2, the NEF determines the PDU session used for the user plane connection between UE and AF.

4. The NEF sends Nsmf_EventExposure_Subscribe to the SMF(s) identified in step 3, including the Target for Event Reporting set to the PDU Session id(s) provided in step 3 and the Event ID set to IP address/prefix allocation/change.

5. The SMF provides the allocated IPv4 address or IPv6 prefix or both to the NEF.

6. The NEF provides the allocated IPv4 address or IPv6 prefix or both provided by SMF in step 5 to the AF.

7. The AF correlates the UE data that includes the UE IP address and the NWDAF request for the GPSI using the retrieved IPv4 address or IP v6 prefix.

If the user plane session between the UE and the AF is released, the AF shall remove the stored correlation information between the UE IP address / prefix and GPSI.

6.2.8.2.4.4 NWDAF correlates UE data collection and NWDAF request for trusted AF and untrusted AF

NWDAF receives the analytics subscription from consumer and discover an AF as described in clause 6.2.8.2.3. NWDAF finds the PDU session(s) serving the SUPI, DNN, S-NSSAI from UDM and the allocated IPv4 address or IPv6 prefix from SMF as described in Figure 6.2.8.2.4.4-1.

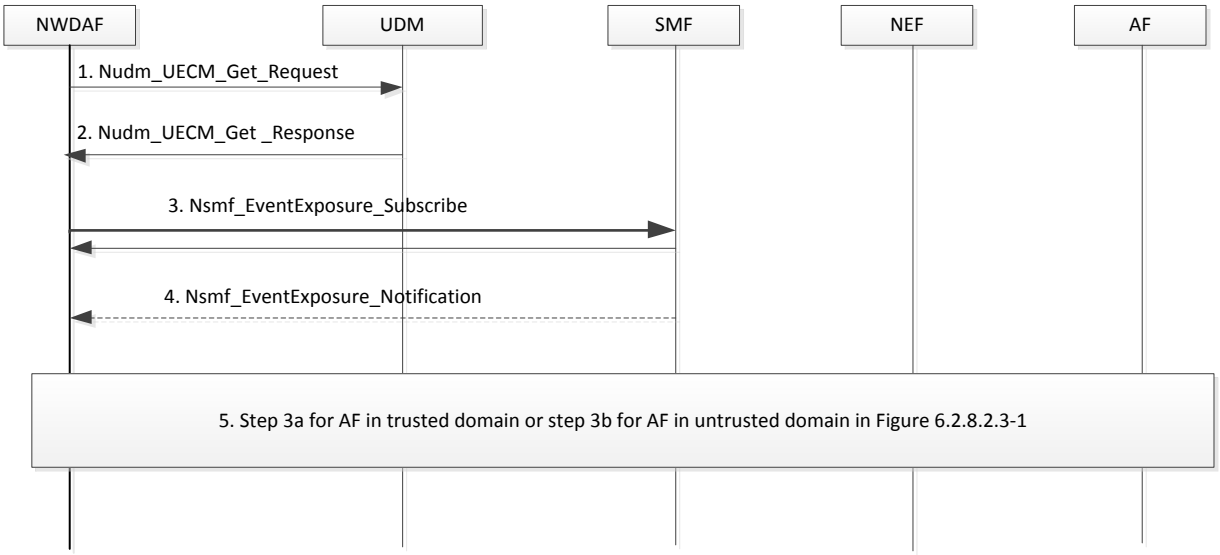

Figure 6.2.8.2.4.4-1: NWDAF correlates UE data collection and NWDAF request

1. The NWDAF finds the SMF(s) serving the PDU session(s) for this SUPI or GPSI using Nudm_UECM_Get_Request including SUPI or GPSI, type of requested information set to SMF Registration Info and the list of S-NSSAI and DNN combinations, as defined in clause 5.3.2.5.7 in TS 29.503 [26]. The NWDAF acquires the DNN, S-NSSAI used to access the AF using Nnrf_NFDiscovery_Request service operation or is configured with the DNN, S-NSSAI used to access the AF.

2. The UDM provides the SMF id(s) and the corresponding PDU Session id(s), per S-NSSAI, DNN combination using Nudm_UECM_Get_Response to the NWDAF. Based on the S-NSSAI, DNN used to access the AF in step 1, NWDAF determines the PDU session used for the user plane connection between UE and AF.

3. The NWDAF sends Nsmf_EventExposure_Subscribe to the SMF identified in step 2, including the Target for Event Reporting set to the PDU Session id(s) provided in step 2 and the Event ID set to IP address/prefix allocation/change.

4. The SMF provides the allocated IPv4 address or IPv6 prefix to the NWDAF.

5. Step 3a for AF in trusted domain or step 3b for AF in untrusted domain in Figure 6.2.8.2.3-1 is performed with the exception that NWDAF sets the allocated IPv4 address or IPv6 prefix that were received in step 4 as target of event reporting.

If NWDAF subscribed for the PDU session used for the user plane connection between the UE and the AF is released notification in step 3, the SMF informs the NWDAF that the UE IP address / prefix is released via Nsmf_EventExposure_Notify. Based on this information, the NWDAF shall remove the stored correlation information between the UE IP address / prefix and SUPI.

6.2.8.2.4a Void

6.2.9 User consent for analytics

Depending on local policy or regulations, to protect the privacy of user data, the data collection, ML model training and analytics generation for a SUPI or GPSI, Internal or External_Group_Id or "any UE" may be subject to user consent

bound to a purpose, such as analytics or ML model training. The user consent is subscription information stored in the UDM, which includes:

a) whether the user authorizes the collection and usage of its data for a particular purpose;

b) the purpose for data collection, e.g., analytics or model training.

The NWDAF retrieves the user consent to data collection and usage from UDM for a user, i.e. SUPI prior to collecting user data from an NF as described in clause 6.2.2 and from a DCCF as described in clause 6.2.6.

If a request for analytics is for "any UE", meaning that the consumer requests analytics for all UEs registered in an area, such as a S-NSSAI or DNN or AoI, then the NWDAF resolves "any UE" into a list of SUPIs using the Namf_EventExposure service with EventId "Number of UEs served by the AMF and located in an area of interest" and retrieves user consent for each SUPI. If a request for analytics is for an Internal or External Group Id, NWDAF resolves it into a list of SUPIs and retrieves user consent for each SUPI.

If user consent for a user is granted, then the NWDAF subscribes to user consent updates in UDM using Nudm_SDM_Subscribe service operation. Otherwise, the NWDAF excludes the corresponding SUPI from the request to collect data and generate analytics or ML model on the other users for which user consent is granted if the request is for a group of UE or "any UE.

When data is collected from the UE Application, the ASP is responsible to obtain user consent to share data with the MNO.

If the UDM notifies that the user consent changed, then the NWDAF checks if the user consent is not granted for the purpose of analytics or model training. If user consent was revoked for a UE, the NWDAF stops data collection for that UE. For analytics subscriptions to UE related analytics with the Target of Analytics Reporting set to that UE, the NWDAF stops generation of new analytics and stops providing affected analytics to consumers. For ML model subscriptions with Target of ML Model Reporting set to that UE, the NWDAF containing MTLF stops (re-)training of ML model(s) using data from the UE and stops providing the ML model(s) to consumers (NWDAF containing AnLF) for analytics. If the Target of Analytics Reporting or Target of ML model Reporting is either an Internal or External Group Id or a list of SUPIs or "any UE", the NWDAF skips those SUPIs that do not grant user consent for the purpose of analytics or model training. The NWDAF may unsubscribe to be notified of user consent updates from UDM for users for which data consent has been revoked.

NOTE: The NWDAF can provide analytics or ML model to consumers that request analytics or ML model for an Internal or External Group Id, or for "any UE", skipping those users for which consent is not granted or is revoked.

The Analytics ID that needs to check user consent before collecting input data are those that collect input data per user, i.e. per SUPI, GPSI, Internal or External Group Id, or those with the Target of Analytics Reporting or Target of ML model Reporting set to a SUPI, GPSI or External or Internal Group Id, and are described in clause 6.

6.2A Procedure for ML Model Provisioning

6.2A.0 General

This clause presents the procedure for the ML Model provisioning.

In this Release of the specification an NWDAF containing AnLF is locally configured with (a set of) IDs of NWDAFs containing MTLF and the Analytics ID(s) supported by each NWDAF containing MTLF to retrieve trained ML models. An NWDAF containing AnLF may use NWDAF discovery for NWDAF containing MTLF within the set of configured IDs of NWDAFs containing MTLF, if necessary. An NWDAF containing MTLF may determine that further training for an existing ML model is needed when it receives the ML model subscription or the ML model request.

NOTE: ML Model provisioning/sharing between multiple MTLFs is not supported in this Release of the specification.

6.2A.1 ML Model Subscribe/Unsubscribe

The procedure in Figure 6.2A.1-1 is used by an NWDAF service consumer, i.e. an NWDAF containing AnLF to subscribe/unsubscribe at another NWDAF, i.e. an NWDAF containing MTLF, to be notified when ML Model

Information on the related Analytics becomes available, using Nnwdaf_MLModelProvision services as defined in clause 7.5. The ML Model Information is used by an NWDAF containing AnLF to derive analytics. The service is also used by an NWDAF to modify existing ML Model Subscription(s). An NWDAF can be at the same time a consumer of this service provided by other NWDAF(s) and a provider of this service to other NWDAF(s).

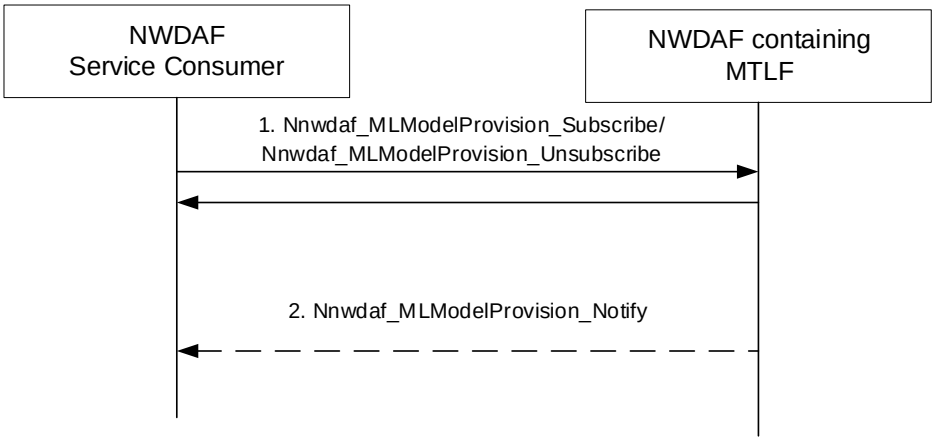

Figure 6.2A.1-1: ML Model for analytics subscribe/unsubscribe

1. The NWDAF service consumer (i.e. an NWDAF containing AnLF) subscribes to, modifies, or cancels subscription for a (set of) trained ML Model(s) associated with a (set of) Analytics ID(s) by invoking the Nnwdaf_MLModelProvision_Subscribe / Nnwdaf_MLModelProvision_Unsubscribe service operation. The parameters that can be provided by the NWDAF service consumer are listed in clause 6.2A.2.

   When a subscription for a trained ML model associated with an Analytics ID is received, the NWDAF containing MTLF may:

   - determine whether an existing trained ML Model can be used for the subscription; or
   - determine whether triggering further training for an existing trained ML models is needed for the subscription.

   If the NWDAF containing MTLF determines that further training is needed, this NWDAF may initiate data collection from NFs, (e.g. AMF/DCCF/ADRF), UE Application (via AF) or OAM as described in clause 6.2, to generate the ML model.

   If the service invocation is for a subscription modification or subscription cancelation, the NWDAF service consumer includes an identifier (Subscription Correlation ID) to be modified in the invocation of Nnwdaf_MLModelProvision_Subscribe.

2. If the NWDAF service consumer subscribes to a (set of) trained ML model(s) associated to a (set of) Analytics ID(s), the NWDAF containing MTLF notifies the NWDAF service consumer with the trained ML Model Information (containing a (set of) file address of the trained ML model) by invoking Nnwdaf_MLModelProvision_Notify service operation. The content of trained ML Model Information that can be provided by the NWDAF containing MTLF is specified in clause 6.2A.2.

   The NWDAF containing MTLF also invokes the Nnwdaf_MLModelProvision_Notify service operation to notify an available re-trained ML model when the NWDAF containing MTLF determines that the previously provided trained ML Model required re-training at step 1.

   When the step 1 is for a subscription modification (i.e., including Subscription Correlation ID), the NWDAF containing MTLF may provide either a new trained ML model different to the previously provided one, or re-trained ML model by invoking Nnwdaf_MLModelProvision_Notify service operation.

6.2A.2 Contents of ML Model Provisioning

The consumers of the ML model provisioning services (i.e. an NWDAF containing AnLF) as described in clause 7.5 and clause 7.6 may provide the input parameters as listed below:

- Information of the analytics for which the requested ML model is to be used, including:

- A list of Analytics ID(s): identifies the analytics for which the ML model is used.
- [OPTIONAL] ML Model Filter Information: enables to select which ML model for the analytics is requested, e.g. S-NSSAI, Area of Interest. Parameter types in the ML Model Filter Information are the same as parameter types in the Analytics Filter Information which are defined in procedures.
- [OPTIONAL] Target of ML Model Reporting: indicates the object(s) for which ML model is requested, e.g. specific UEs, a group of UE(s) or any UE (i.e. all UEs).
- ML Model Reporting Information with the following parameters:
  - (Only for Nnwdaf_MLModelProvision_Subscribe) ML Model Reporting Information Parameters as per Event Reporting Information Parameter defined in Table 4.15.1-1, TS 23.502 [3].
- [OPTIONAL] ML Model Target Period: indicates time interval [start, end] for which ML model for the Analytics is requested. The time interval is expressed with actual start time and actual end time (e.g. via UTC time).
- A Notification Target Address (+ Notification Correlation ID) as defined in TS 23.502 [3] clause 4.15.1, allowing to correlate notifications received from the NWDAF containing MTLF with this subscription.

The NWDAF containing MTLF provides to the consumer of the ML model provisioning service operations as described in clause 7.5 and 7.6, the output information as listed below:

- (Only for Nnwdaf_MLModelProvision_Notify) The Notification Correlation Information.
- ML Model Information, which includes the ML model file address (e.g. URL or FQDN) for the Analytics ID(s).
- [OPTIONAL] Validity period: indicates time period when the provided ML Model Information applies.
- [OPTIONAL] Spatial validity: indicates Area where the provided ML Model Information applies.

NOTE: Spatial validity and Validity period are determined by MTLF internal logic and it is a subset of AoI if provided in ML Model Filter Information and of ML Model Target Period, respectively.

6.2A.3 ML Model request

The procedure in Figure 6.2A.3-1 is used by an NWDAF service consumer, i.e. an NWDAF containing AnLF to request and get from another NWDAF, i.e. an NWDAF containing MTLF ML Model Information, using Nnwdaf_MLModelInfo services as defined in clause 7.6. The ML Model Information is used by an NWDAF containing AnLF to derive analytics. An NWDAF can be at the same time a consumer of this service provided by other NWDAF(s) and a provider of this service to other NWDAF(s).

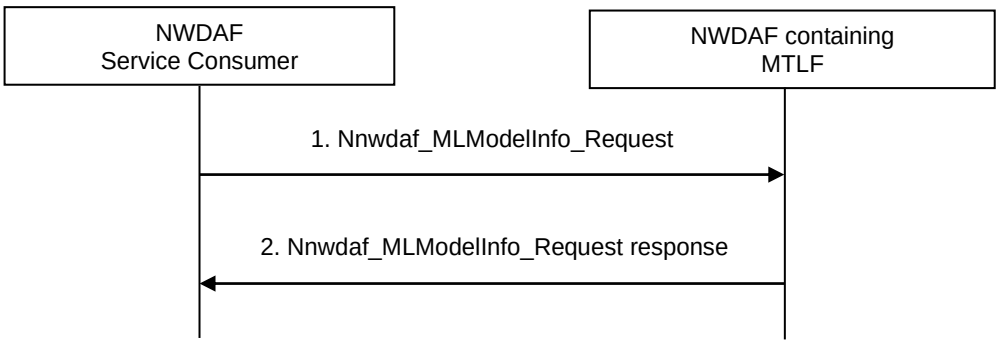

Figure 6.2A.3-1: ML model Request

1. The NWDAF service consumer (i.e., an NWDAF containing AnLF) requests a (set of) ML Model(s) associated with a (set of) Analytics ID(s) by invoking Nnwdaf_MLModelInfo_Request service operation. The parameters that can be provided by the NWDAF Service Consumer are listed in clause 6.2A.2.

   When a request to an ML Model Information for the Analytics is received, the NWDAF containing MTLF may:

- determine whether an existing trained ML Model can be used for the request; or
- determine whether triggering further training for an existing trained ML models is needed for the request.

If the NWDAF containing MTLF determines that further training is needed, this NWDAF may initiate data collection from NFs, (e.g. AMF/DCCF/ADRF), UE Application (via AF) or OAM as described in clause 6.2, to generate the ML model.

2. The NWDAF containing MTLF responds with the ML Model Information (containing a (set of) file address of the trained ML model) to the NWDAF service consumer by invoking Nnwdaf_MLModelInfo_Request response service operation. The content of ML Model Information that can be provided by the NWDAF containing MTLF is specified in clause 6.2A.2.

6.2B Analytics Data Repository procedures

6.2B.1 General

Collected data and analytics may be stored in ADRF, using procedure as specified in clause 6.2B.2 and clause 6.2B.3. Collected data and analytics may be deleted from ADRF, using procedure as specified in clause 6.2B.4.

6.2B.2 Historical Data and Analytics storage

The procedure depicted in figure 6.2B.2-1 is used by consumers (e.g. NWDAF, DCCF or MFAF) to store historical data and/or analytics, i.e. data and/or analytics related to past time period that has been obtained by the consumer. After the consumer obtains data and/or analytics, consumer may store historical data and/or analytics in an ADRF. Whether the consumer directly contacts the ADRF or goes via the DCCF or via the Messaging Framework is based on configuration.

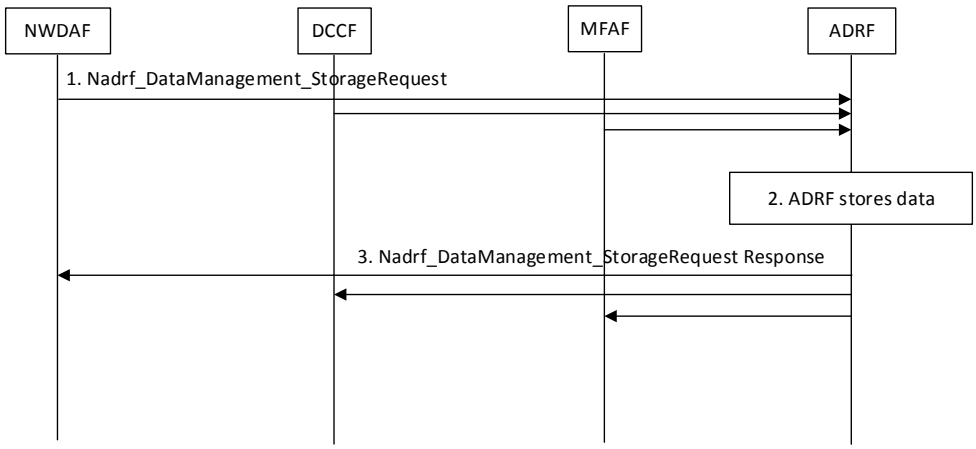

Figure 6.2B.2-1: Historical Data and Analytics storage

1. The consumer sends data and/or analytics to the ADRF by invoking the Nadrf_DataManagement_StorageRequest (collected data, analytics) service operation.
2. The ADRF stores the data and/or analytics sent by the consumer. The ADRF may, based on implementation, determines whether the same data and/or analytics is already stored or being stored based on the information sent in step 1 by the consumer NF and, if the data and/or analytics is already stored or being stored in the ADRF, the ADRF decides to not store again the data and/or analytics sent by the consumer.
3. The ADRF sends Nadrf_DataManagement_StorageRequest Response message to the consumer indicating that data and/or analytics is stored, including when the ADRF may have determined at step 2 that data or analytics is already stored.

6.2B.3 Historical Data and Analytics Storage via Notifications

The procedure depicted in figure 6.2B.3-1 is used by consumers (NWDAF, DCCF) to store received notifications in the ADRF. The consumer requests the ADRF to initiate a subscription for data and/or analytics. Data and/or analytics provided in notifications as a result of the subsequent subscription by the ADRF are stored in the ADRF.

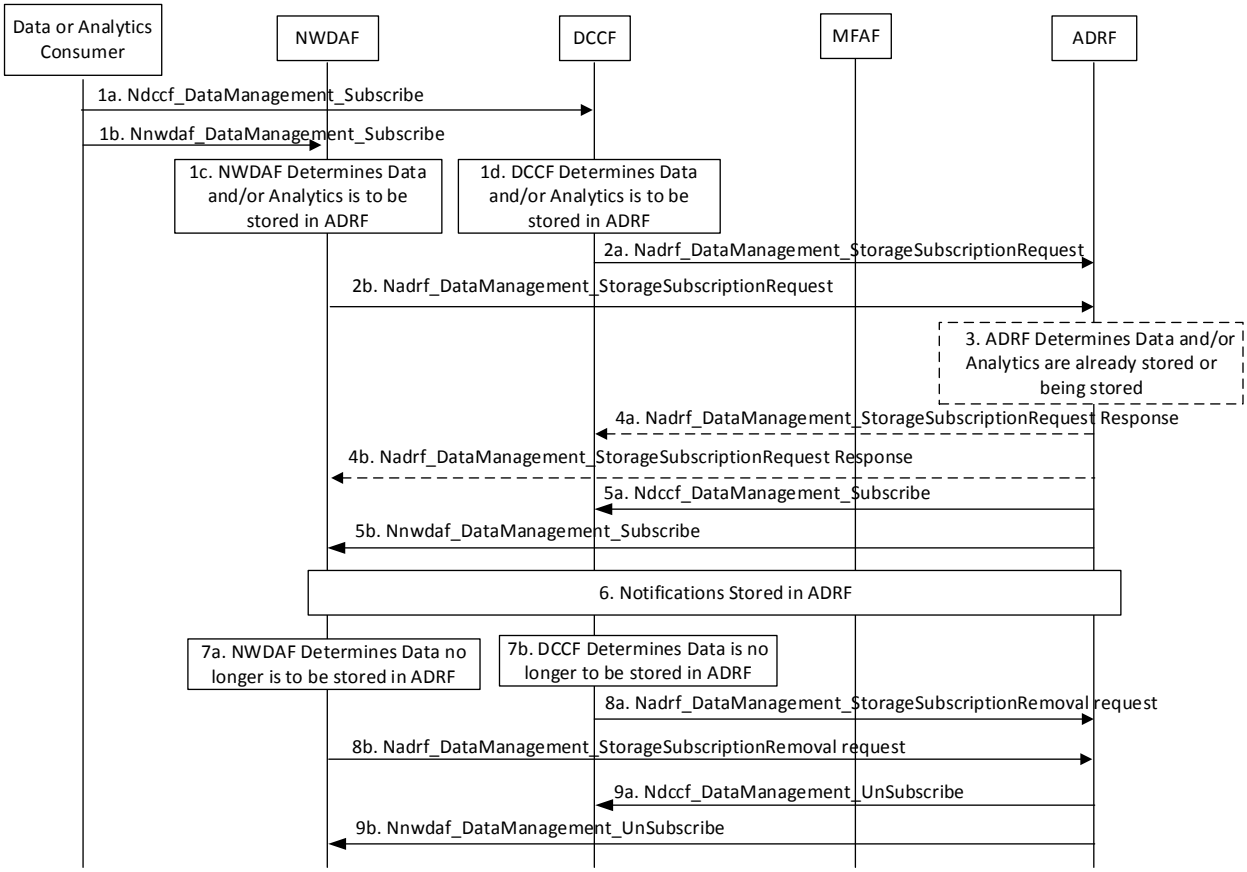

Figure 6.2B.3-1: Historical Data and Analytics Storage via Notifications

1a-d. Based on provisioning or based on reception of a DataManagement subscription request (e.g. see clause 6.2.6.3.2), the DCCF or the NWDAF determines that notifications are to be stored in an ADRF.

2a-b. The DCCF or the NWDAF determines the ADRF where data and/or analytics needs to be stored, and requests that the ADRF subscribes to receive notifications. The determination may be made based on configuration or information supplied by the data consumer as described in clauses 6.1.4 and 6.2.6.3. The request to the ADRF specifies the data and/or analytics to which the ADRF will subscribe by invoking the Nadrf_DataManagement_StorageSubscriptionRequest service operation.

3. [Optional] The ADRF may, based on implementation, determines whether the same data and/or analytics is already stored or being stored, based on the information sent in step 2 by the consumer.

4. [Optional] If the data and/or analytics is already stored and/or being stored in the ADRF, the ADRF sends Nadrf_DataManagement_StorageRequest Response message to the consumer indicating that data and/or analytics is stored.

5a-b. ADRF subscribes to the DCCF or the NWDAF to receive notifications, providing its notification endpoint address and a notification correlation ID.

6. The DCCF, the MFAF or the NWDAF send Analytics or Data notifications containing the notification correlation ID provided by the ADRF to ADRF notification endpoint address. The ADRF stores the notifications.

7a-b. The DCCF or the NWDAF determines that notifications no longer need to be stored in the ADRF.

8a-b. The DCCF or the NWDAF requests that the ADRF unsubscribes to receive notifications.

9a-b. The ADRF sends a request to the DCCF or the NWDAF to unsubscribe to data notifications.

The NWDAF may interact with the Data Source, and the DCCF may interact with the Data Source and/or MFAF. Delivery notifications from the DCCF/MFAF or NWDAF to the ADRF are subsequently halted.

6.2B.4 Data removal from an ADRF

The procedure depicted in figure 6.2B.4-1 is used by consumers (DCCF, NWDAF) to remove data previously stored in an ADRF.

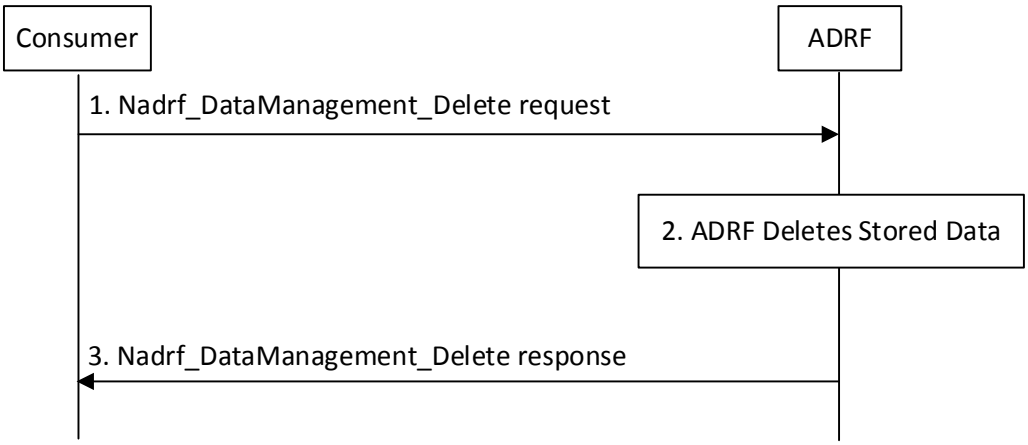

Figure 6.2B.4-1: Data Removal from an ADRF

1. A consumer requests that specified data be deleted from the ADRF using Nadrf_DataManagement_Delete request service operations.
2. The ADRF deletes all copies of the stored data.
3. The ADRF indicates the result (i.e. data deleted, data not found, data found but not deleted) using Nadrf_DataManagement_Delete response service operations.

6.3 Slice load level related network data analytics

6.3.1 General

The NWDAF provides slice load level information to a consumer NF on a Network Slice level or a Network Slice instance level or both. The NWDAF is not required to be aware of the current subscribers using the slice. The NWDAF notifies slice specific network status analytics information to the consumer NF that is subscribed to it. A consumer NF may collect directly slice specific network status analytics information from NWDAF. This information is not subscriber specific.

The NWDAF services as defined in the clause 7.2 and clause 7.3 are used to expose slice load level analytics from the NWDAF to the consumer NF (e.g. PCF, NSSF or AMF).

The consumer of these analytics shall indicate in the request or subscription:

- Analytics ID = "Load level information";
- Analytics Filter Information:
  - S-NSSAI and NSI ID;
  - optionally, the list of analytics subsets that are requested among those specified in clause 6.3.3A;

NOTE: The use of NSI ID in the network is optional and depends on the deployment choices of the operator. If used, the NSI ID is associated with S-NSSAI. NSI ID is only applicable when the consumer of analytics is NSSF or AMF.

- an optional Area of Interest;
- an optional list of NF types;
- optionally, Load Level Threshold value; and
- optionally, "maximum number of objects" indicating the maximum number of Network Slice instances expected in output, when the Analytics Filter Information does not indicate an NSI ID.

6.3.2 Void

6.3.2A Input data

The detailed information collected by the NWDAF is listed in Table 6.3.2A-1 and Table 6.3.2A-2.

Table 6.3.2A-1: OAM Input data for slice load analytics

Information	Source	Description
UE registered in a Network Slice/Network Slice instance	OAM	Mean number of UEs registered in a NW slice or NW slice instance as defined in TS 28.552 [8]. (NOTE 1).
PDU Session established on a Network Slice/Network Slice instance	OAM	Mean number of established PDU Sessions in a NW slice or NW slice instance as defined in TS 28.552 [8]. (NOTE 1).
Load of NFs associated to Network Slice instance	OAM	Resource utilization information of a Network Slice instance obtained from its constituent NF instances. NF instance load input data collection is described in clause 6.5, Table 6.5.2-1.
NOTE 1: 5GC performance measurements can be provided per S-NSSAI by OAM as defined in TS 28.552 [8]. Any 5GC performance measurements per NSI ID required further coordination with SA WG5.		

Table 6.3.2A-2: 5GC NF Input data for slice load analytics

Information	Source	Description
Timestamps	5GC NF	A time stamp associated with the collected information.
UE registers/de-registers to a Network Slice/Network Slice instance	AMF(s)	AMF reports that a UE registered or deregistered to a S-NSSAI or to a S-NSSAI and NSI ID.
Number of UEs served by the AMF	AMF(s)	AMF reports the total number of UEs served by the AMF per S-NSSAI or per S-NSSAI and NSI ID. (NOTE 1)
PDU Session established/released on a Network Slice	SMF(s)	SMF reports that a PDU Session is established or released per S-NSSAI or per S-NSSAI and NSI ID.
Current number of UEs registered in a NW slice	NSACF	NSACF reports the number of UE registered at the S-NSSAI.
Current number of PDU Sessions established in a NW slice	NSACF	NSACF reports the number of PDU Sessions established at the S-NSSAI.
Load of NFs associated to Network Slice instance	NRF	Resource utilization information of a Network Slice instance obtained from its constituent NF instances. NF instance load input data collection is described in clause 6.5, Table 6.5.2-1.
NOTE 1: AMF reports the total number of registered UE in the AMF at each associated time stamp. NOTE 2: SMF reports multiple PDU Sessions when establishment or release happened at the same time, indicated by the time stamp. NOTE 3: Based on the internal logic, the NWDAF determines the source for the data collection.		

NWDAF collects input data on the number of UEs registered in a S-NSSAI or S-NSSAI and NSI ID combination using one of the following options:

- Total number of UE registered to a S-NSSAI or to a S-NSSAI and NSI ID from each AMF(s) and/or from NSCAF:
  - Namf_EventExposure_Subscribe (Target for Event Reporting = "any UE", Event ID = "Number of UEs served by the AMF and located in "Area of Interest"", Event Filter information = S-NSSAI(s) or one or more of the tuple (S-NSSAI, NSI ID), Event reporting mode = periodic along with periodicity) as defined in clause 5.2.2.3.1 of TS 23.502 [3]; or
  - Nnsacf_SliceEventExposure_Subscribe (EventID = "Number of UE registered", EventFilter = "S-NSSAI", Event reporting mode = periodic along with periodicity) as defined in clause 5.2.21.4.2 of TS 23.502 [3].
- Individual UE registration/deregistration to a S-NSSAI or to a S-NSSAI and NSI ID reported by AMF(s):
  - Namf_EventExposure_Subscribe (Target for Event Reporting = "any UE", Event ID = "UE moving in or out of a subscribed "Area of Interest", Event Filter information = S-NSSAI(s) or one or more of the tuples (S-NSSAI, NSI ID), Event reporting mode = reporting to a maximum number or a maximum duration) as defined inclause 5.2.2.3.1 of TS 23.502 [3].

NWDAF collects input data on the number of PDU Sessions established in a S-NSSAI using one of the following options:

- Total number of PDU Sessions established in a S-NSSAI from each SMF(s) and/or NSACF:
  - Nnsacf_SliceEventExposure_Subscribe (EventID = "Number of PDU sessions established", EventFilter = "S-NSSAI(s)", Event reporting mode = periodic along with periodicity) as defined in clause 5.2.21.4.2 of TS 23.502 [3].
- Individual PDU Session Established or PDU Session Released in a S-NSSAI from SMF:
  - Nsmf_EventExposure_Subscribe (Target for Event Reporting = "any UE", Event ID = "PDU Session Establishment and/or PDU Session Release", Event Filter information = S-NSSAI(s), Event reporting mode = reporting to a maximum number or a maximum duration) as defined inclause 5.2.8.3.1 of TS 23.502 [3].

6.3.3 Void

6.3.3A Output analytics

The NWDAF services as defined in the clause 7.2 and 7.3 are used to expose the following analytics:

- Network Slice instance load statistics information as defined in Table 6.3.3A-1.
- Network Slice load statistics information as defined in Table 6.3.3A-2.
- Network Slice instance load predictions information as defined in Table 6.3.3A-3.
- Network Slice load predictions information as defined in Table 6.3.3A-4.

Table 6.3.3A-1: Network Slice instance load statistics

Information	Description
S-NSSAI	Identification of the Network Slice.
Network Slice instances (1..max)	List of Network Slice instance(s) within the S-NSSAI.
> NSI ID	Identification of the Network Slice instance.
> Number of UE Registrations (NOTE 1)	Number of UE registrations of the Network Slice instance(average, variance).
> Number of PDU Sessions establishment(NOTE 1)	Number of PDU Session establishments of the Network Slice instance(average, variance).
> Resource usage (NOTE 1)	The usage of assigned virtual resources currently in use for the NF instances (mean usage of virtual CPU, memory, disk) as defined in TS 28.552 [8] clause 5.7, belonging to a particular Network Slice instance.
> Resource usage threshold crossings (NOTE 1)	Number of times resource usage threshold is met or exceeded or crossed on the Network Slice instance provided if threshold is provided by the consumer as Analytics Filter.
> Resource usage threshold crossings time period (1..max)(NOTE 1)	Resource usage threshold crossing vector including time elapsed between times each threshold is met or exceeded or crossed on the Network Slice instance provided that a threshold value is provided by the consumer as Analytics Filter.
> Load Level (NOTE 1)	The load level of the Network Slice Instance indicated by the S-NSSAI and the associated NSI ID (if applicable) in the Analytics Filter, if Load Level Threshold is not provided by the consumer as Analytics Filter.
> Crossed Load Level Threshold (NOTE 1)	The Load Level Threshold that are met or exceeded by the statistics value of the Load Level if the Load Level Threshold is provided by the consumer as Analytics Filter.
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested".	

Table 6.3.3A-2: Network Slice load statistics

Information	Description
S-NSSAI	Identification of the Network Slice.
> Number of UE Registrations (NOTE 1)	Number of UE registrationsat the Network Slice(average, variance).
>Number of PDU sessions establishments (NOTE 1)	Number of PDU Session establishmentsat the Network Slice(average, variance).
> Load Level (NOTE 1)	The load level of the Network Slice Instance indicated by the S-NSSAI and the associated NSI ID (if applicable) in the Analytics Filter, if Load Level Threshold is not provided by the consumer as Analytics Filter.
> Crossed Load Level Threshold (NOTE 1)	The Load Level Threshold that are met or exceeded by the statistics value of the Load Level if the Load Level Threshold is provided by the consumer as Analytics Filter.
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested".	

Table 6.3.3A-3: Network Slice instance load predictions

Information	Description
S-NSSAI	Identification of the Network Slice.
Network Slice instances (1..max)	List of Network Slice instance(s) within the S-NSSAI.
> NSI ID	Identification of the Network Slice instance.
> Number of UE Registrations (NOTE 1)	Number of predicted UE registrationsat the Network Slice instance (average, variance).
> Number of PDU Sessions establishment(NOTE 1)	Number of predicted PDU Session establishments of the Network Slice instance (average, variance).
> Resource usage (NOTE 1)	The predicted usage of assigned virtual resources for the NF instances (mean usage of virtual CPU, memory, disk) as defined in TS 28.552 [8] clause 5.7, belonging to a particular Network Slice instance.
> Resource usage threshold crossings (NOTE 1)	Number of predicted timesresource usage threshold is met or exceeded or crossed at the Network Slice instance provided that a threshold value is provided by the consumer as Analytics Filter.
> Resource usage threshold crossings time period (1..max) (NOTE 1)	Predicted Resource usage threshold vector including predicted time elapsed between times each threshold is met or exceeded or crossed on the Network Slice instance provided that a threshold value is provided by the consumer as Analytics Filter.
> Load Level (NOTE 1)	The load level of the Network Slice Instance indicated by the S-NSSAI and the associated NSI ID (if applicable) in the Analytics Filter, if Load Level Threshold is not provided by the consumer as Analytics Filter.
> Crossed Load Level Threshold (NOTE 1)	The Load Level Threshold that are met or exceeded by the predicted value of the Load Level if the Load Level Threshold is provided by the consumer as Analytics Filter.
> Confidence	Confidence of this prediction.
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested".	

Table 6.3.3A-4: Network Slice load predictions

Information	Description
S-NSSAI	Identification of the Network Slice.
> Number of UE Registrations(NOTE 1)	Predicted Number of UE registrationsat the Network Slice (average, variance).
>Number of PDU sessions establishments (NOTE 1)	Predicted Number of PDU Session establishmentsat the Network Slice (average, variance).
> Load Level (NOTE 1)	The load level of the Network Slice Instance indicated by the S-NSSAI and the associated NSI ID (if applicable) in the Analytics Filter, if Load Level Threshold is not provided by the consumer as Analytics Filter.
> Crossed Load Level Threshold (NOTE 1)	The Load Level Threshold that are met or exceeded by the predicted value of the Load Level if the Load Level Threshold is provided by the consumer as Analytics Filter.
> Confidence	Confidence of this prediction.
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested".	

NOTE: If no NSI ID is provided as Analytics Filter, slice load level related output analytics are provided according to Tables 6.3.3A-2 and 6.3.3A-4. Otherwise slice instance load level related output analytics are provided according to Tables 6.3.3A-1 and 6.3.3A-3.

6.3.4 Procedures

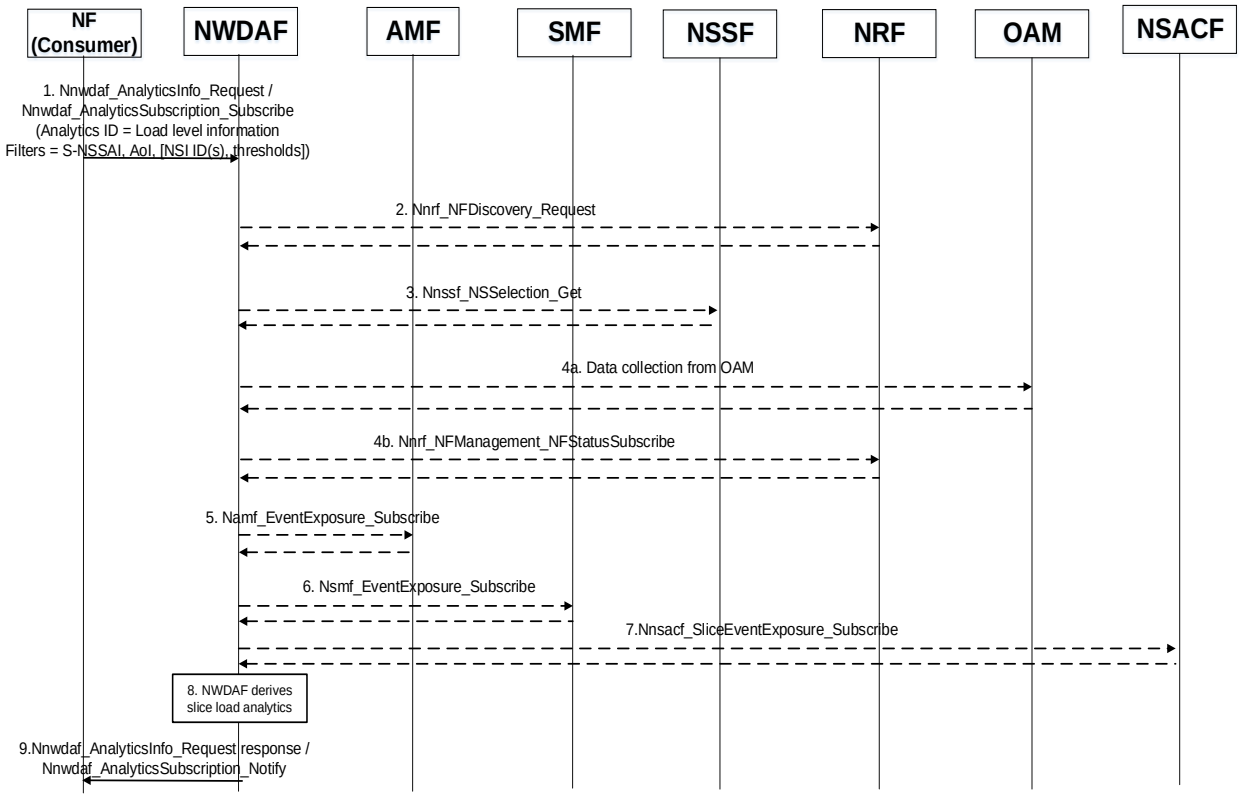

Figure 6.3.4-1: Network Slice load analytics provided by NWDAF

Figure 6.3.4-1 shows the procedure for NWDAF to derive slice load analytics. The steps are described as follows:

1. A consumer NF subscribes to/requests a NWDAF using Nnwdaf_AnalyticsSubscription_Subscribe or Nnwdaf_AnalyticsInfo_Request service operation (Analytics ID = Load level information and a set of Analytics Filters (e.g. S-NSSAI, NSI ID, Area of Interest)).

2. [OPTIONAL] If the NWDAF does not have already the slice information, it gains the slice information from OAM (as described in clause 6.2.3) and discovers from NRF the AMF, SMF and NSSF instance(s) relevant to the Analytics Filters provided in the analytics subscription.

3. [OPTIONAL] If the NSI ID(s) are not provided in the analytics subscription by the consumer NF, the NWDAF invokes Nnssf_NSSelection_Get service operation from NSSF to obtain the NSI ID(s) corresponding to the S-NSSAI in the subscription.

NOTE: Step 4a to step 7 are conditional depending on the NWDAF internal logic that determines the source(s) of data collection.

4a. [CONDITIONAL] The NWDAF may subscribe to input data in Table 6.3.2A-1 from the OAM according to the data collection principles from the OAM described in clause 6.2.3.

4b. [CONDITIONAL] The NWDAF may collect input data from the NRF (see clause 6.5) to derive slice instance resource usage statistics and predictions for a Network Slice instance.

5. [CONDITIONAL] The NWDAF may subscribe to the AMF(s) event exposure service to collect data on the number of UEs currently registered on certain Network Slice and, if available, its constituent Network Slice instance(s) as defined in clause 6.3.2A. If required, the NWDAF may also collect the corresponding UE IDs.

6. [CONDITIONAL] The NWDAF may subscribe to the SMF(s) event exposure service to collect data on the number of PDU sessions established and/or released at the SMF on currently registered on certain Network Slice as defined in clause 6.3.2A. NWDAF can then use such collected data to determine the number of PDU sessions

established on i) a Network Slice; and ii) if available, on a Network Slice instance by leveraging the data collected in step 5.

7. [CONDITIONAL] The NWDAF may subscribe to one or multiple NSACFs to collect data on either the number of UE registered in a S-NSSAI or the number of PDU sessions established in a S-NSSAI as defined in clause 6.3.2A. When multiple NSACFs are selected by the NWDAF for the S-NSSAI, the NWDAF aggregates the reports from the NSACFs to derive the number of UEs registered in the S-NSSAI or the number of PDU sessions established in the S-NSSAI.

8. The NWDAF derives slice load analytics.

9. The NWDAF delivers analytics to the consumer NF by invoking Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response service operations.

6.4 Observed Service Experience related network data analytics

6.4.1 General

This clause specifies how NWDAF can provide Observed Service Experience (i.e. average of observed Service MoS and/or variance of observed Service MoS indicating service MOS distribution for services such as audio-visual streaming as well as services that are not audio-visual streaming such as V2X and Web Browsing services) analytics, in the form of statistics or predictions, to a service consumer.

The Observed Service Experience analytics may provide one or more of the following outputs:

- Service Experience for a Network Slice: Service Experiencefor a UE or a group of UEs or any UE in a Network Slice;

- Service Experience for an Application: Service Experience for a UE or a group of UEs or any UE in an Application or a set of Applications;

- Service Experience for an Edge Application over a UP path: Service experience for a UE or a group UEs or any UE in an Application or a set of Applications over a specific UP path (UPF, DNAI and EC server);

- Service Experience for an Application over a RAT Type or Frequency or both: Service experience for a UE or a group of UEs in an Application or a set of Applications over a RAT Type or over a Frequency or both as defined in Table 6.4.1-1.

Therefore, Observed Service experience may be provided as defined in clause 6.4.3. For example, individually per UE or group of UEs, or globally, averaged per Application or averaged across a set of Applications on a Network Slice.

The service consumer may be an NF (e.g. PCF, NSSF, AMF), AF, or the OAM.

The consumer of these analytics shall indicate in the request or subscription:

- Analytics ID = "Service Experience";

- Target of Analytics Reporting: one or more SUPI(s) or Internal Group Identifier(s), or "any UE";

- Analytics Filter Information as defined in Table 6.4.1-1;

- optionally, maximum number of objects and maximum number of SUPIs;

- optionally, preferred level of accuracy of the analytics;

- optionally, a list of analytics subsets that are requested (see clause 6.4.3)

- optionally, preferred level of accuracy per analytics subset;

- optionally, preferred order of results for the list of Application Service Experiences and/or Slice instance service experiences: "ascending" or "descending"; and

- optionally, preferred granularity of location information: TA level or cell level.

Table 6.4.1-1: Analytics Filter Information related to the observed service experience

Information	Description	Mandatory			
		Application	Network Slice	Edge Applications over a UP path	Application over RAT Type and frequency
Application ID (0...max)	The identification of the application(s) for which the analytics information is subscribed or requested.	Y	N	Y	Y
S-NSSAI	When requesting Service Experience for a Network Slice: identifies the Network Slice for which analytics information is subscribed or requested. When requesting Service Experience for an Application: identifies the S-NSSAI used to access the application together with the DNN listed below.	N	Y	N	N
NSI ID(s)	Identifies the Network Slice instance(s) for which analytics information is subscribed or requested.	N	N	N	N
Area of Interest	Identifies the Area (i.e. set of TAIs), as defined in TS 23.501 [2] for which the analytics information is subscribed or requested.	N	N	N	N
DNN	When requesting Service Experience for an Application, this is the DNN to access the application.	N	N	N	N
DNAI (NOTE 1)	Identifier of a user plane access to one or more DN(s) where applications are deployed as defined in TS 23.501 [2].	N	N	Y	N
RAT Type (NOTE 2)	Identifies the RAT type.	N	N	N	Y
Frequency (NOTE 2)	Identifies the Frequency value(s) (e.g. high, low).	N	N	N	Y
Application Server Address(es) (NOTE 1)	List of IP address(s)/FQDN(s) of the Application Server(s) that a UE, group of UEs, or 'any UE' has a communication session for which Service Experience Analytic information is requested.	N	N	Y	N
UPF anchor ID (NOTE 1)	Identifies the UPF where a UE has an associated PDU session	N	N	N	N
NOTE 1: These parameters can be provided when a consumer requires analytics for an edge application over a UP path. NOTE 2: A service consumer can provide either a RAT Type or a Frequency or a specific combination of RAT Type and Frequency. A service consumer can also provide multiple instances of RAT Type or multiple instances of Frequency or multiple combinations of RAT type and Frequency. A service consumer can also provide "any" RAT type indication "any" Frequency value indication or "any" indication for all the RAT type and Frequency value the NWDAF has received for the application.					

NOTE: A service consumer can use the Area of Interest in order to reduce the amount of signalling that the analytics subscription or request generates.

- An Analytics target period that indicates the time window for which the statistics or predictions are requested;
- In a subscription, the Notification Correlation Id and the Notification Target Address;
- Optionally, Reporting Thresholds, which apply only for subscriptions and indicate conditions on the Service Experience to be reached in order to be notified by the NWDAF (see Table 6.4.3-1 and Table 6.4.3-2).

The NWDAF shall notify the result of the analytics to the consumer as specified in clause 6.4.3.

NWDAF collects the network data from AF (directly or via NEF) and from other 5GC NF(s) in order to calculate and provide statistics and predictions on the observed service experience to a consumer NF or to OAM.

Based on the Analytics Filter information in Table 6.4.1-1 and the Target of Analytics Reporting provided by the service consumer in the analytics subscription or request, NWDAF determines whether service experience analytics should be delivered for:

i) Application(s);

ii) Network Slice;

iii) both Application(s) and Network Slice;

iv) Edge Applications over a UP path;

v) Application(s) over RAT Type(s) and/or Frequency value(s).

If NWDAF is unable to differentiate based on the analytics subscription or request, it provides service experience analytics for both Application(s) and Network Slice.

If service experience for both Application(s) and Network Slice is desired but the Target of Analytics Reporting or Analytics Filter information values (e.g. Area of Interest) need to be different, separate subscriptions/requests may be provided by the service consumer.

6.4.2 Input Data

The service data and performance data collected from the AF (including the service data collected from the UE through the AF), the network data from other 5GC NFs and the network data from OAM for observed service experience are defined in Table 6.4.2-1, 6.4.2-1a, Table 6.4.2-2, Table 6.4.2-3 and Table 6.4.2-4 respectively.

Table 6.4.2-1: Service Data from AF related to the observed service experience

Information	Source	Description
Application ID	AF	To identify the service and support analytics per type of service (the desired level of service)
IP filter information	AF	Identify a service flow of the UE for the application
Locations of Application	AF/NEF	Locations of application represented by a list of DNAI(s). The NEF may map the AF-Service-Identifier information to a list of DNAI(s) when the DNAI(s) being used by the application are statically defined.
Service Experience	AF	Refers to the QoE per service flow as established in the SLA and during on boarding. It can be either e.g. MOS or video MOS as specified in ITU-T P.1203.3 [11] or a customized MOS for any kind of service including those not related to video or voice.
QoE metrics	UE (via AF)	QoE metrics observed at the UE(s). QoE metrics and measurement as described in TS 26.114 [27], TS 26.247 [28], TS 26.118 [29], TS 26.346 [30], TS 26.512 [31] or ASP specific QoE metrics, as agreed in the SLA with the MNO, may be used. Editor's note: How to structure the ASP specific QoE metrics and which specification will document it depends on SA WG4's decision.
Timestamp	AF	A time stamp associated to the Service Experience provided by the AF, mandatory if the Service Experience is provided by the ASP.
Application Server Instance	AF	The IP address or FQDN of the Application Server that the UE had a communication session when the measurement was made.

NWDAF subscribes to the service data from AF in the Table 6.4.2-1 either directly for trusted AFs by invoking Naf_EventExposure_Subscribe service (Event ID = Service Experience information, Event Filter information = Area of Interest, Application ID) as defined in TS 23.502 [3], or indirectly for untrusted AFs via NEF by invoking Nnef_EventExposure_Subscribe service (Event ID = Service Experience information, Event Filter information = Area

of Interest, Application ID) where NEF translates the Area of Interest into geographic zone identifier(s). For the information whose source is UE (via AF), the AF collects data from the UE as defined in clause 6.2.8.

NOTE: When the Service Experience is expressed as a customized MOS, the customized MOS might be defined by the content provider or by the MNO and might be based on the nature of the targeted service type (e.g. web browsing, gaming, augmented reality, V2X, SMS).

Table 6.4.2-1a: Performance Data from AF

Information	Source	Description
UE identifier	AF	IP address of the UE at the time the measurements was made.
UE location	AF	The location of the UE when the performance measurement was made.
Application ID	AF	To identify the service and support analytics per type of service (the desired level of service).
IP filter information	AF	Identify a service flow of the UE for the application.
Locations of Application	AF/NEF	Locations of application represented by a list of DNAI(s). The NEF may map the AF-Service-Identifier information to a list of DNAI(s) when the DNAI(s) being used by the application are statically defined.
Application Server Instance address	AF/NEF	The IP address/FQDN of the Application Server that the UE had a communication session when the measurement was made.
Performance Data	AF	The performance associated with the communication session of the UE with an Application Server that includes: Average Packet Delay, Average Loss Rate and Throughput.
Timestamp	AF	A time stamp associated to the Performance Data provided by the AF.

NWDAF subscribes to the performance data from AF in the Table 6.4.2-1a either directly for trusted AFs by invoking Naf_EventExposure_Subscribe service (Event ID = Performance Data, Event Filter information = Area of Interest, Application ID) as defined in TS 23.502 [3], or indirectly for untrusted AFs via NEF by invoking Nnef_EventExposure_Subscribe service (Event ID = Performance Data, Event Filter information = Area of Interest, Application ID) where NEF translates the Area of Interest into geographic zone identifier(s).

Table 6.4.2-2: QoS flow level Network Data from 5GC NF related to the QoS profile assigned for a particular service (identified by an Application Id or IP filter information)

Information	Source	Description
Timestamp	5GC NF	A time stamp associated with the collected information.
Location	AMF	The UE location information, e.g. cell ID or TAI.
UE ID	AMF	(list of) SUPI(s). If UE IDs are not provided as Target of Analytics Reporting for slice service experience, AMF returns the UE IDs matching the AMF event filters.
DNN	SMF	DNN for the PDU Session which contains the QoS flow.
S-NSSAI	SMF	S-NSSAI for the PDU Session which contains the QoS flow.
Application ID	SMF	Used by NWDAF to identify the application service provider and application for the QoS flow.
UPF info (NOTE 1)	SMF	UPF ID/address/FQDN information for the UPF serving the UE.
DNAI	SMF	Identifies the access to DN to which the PDN session connects.
IP filter information	SMF	Provided by the SMF, which is used by NWDAF to identify the service data flow for policy control and/or differentiated charging for the QoS flow.
QFI	SMF	QoS Flow Identifier.
QoS flow Bit Rate	UPF	The observed bit ratefor UL direction; and The observed bit rate for DL direction.
QoS flow Packet Delay	UPF	The observed Packet delay for UL direction; and The observed Packet delay for the DL direction.
Packet transmission	UPF	The observed number of packet transmission.
Packet retransmission	UPF	The observed number of packet retransmission.
NOTE 1: The UPF info may indicate information of an anchor UPF of the PDU session containing the QoS flow.		

NOTE 1: How NWDAF collects QoS flow Bit Rate, QoS flow Packet Delay, Packet transmission and Packet retransmission information from UPF is not defined in this Release of the specification.

NOTE 2: Care needs to be taken with regards to load and major signalling caused when requesting Any UE. This could be achieved via utilization of some event filters (e.g. Area of Interest for AMF), Analytics Reporting Information (e.g. SUPImax), or sampling ratio as part of Event Reporting Information.

NWDAF subscribes to the network data from 5GC NF(s) in the Table 6.4.2-2 by invoking Nnf_EventExposure_Subscribe service operation with the following Event IDs as input parameters:

- AMF Source: Namf_EventExposure_Subscribe (Event IDs = Location Changes, Area of Interest).
- SMF Source: Nsmf_EventExposure_Subscribe (Event ID = QFI allocation).

Table 6.4.2-3: UE level Network Data from OAM related to the QoS profile

Information	Source	Description
Timestamp	OAM	A time stamp associated with the collected information.
Reference Signal Received Power	OAM (see NOTE 1)	The per UE measurement of the received power level in a network cell, including SS-RSRP, CSI-RSRP as specified in clause 5.5 of TS 38.331 [14] and E-UTRA RSRP as specified in clause 5.5.5 of TS 36.331 [15]
Reference Signal Received Quality	OAM (see NOTE 1)	The per UE measurement of the received quality in a network cell, including SS-RSRQ, CSI-RSRQ as specified in clause 5.5 of TS 38.331 [14] and E-UTRA RSRQ as specified in clause 5.5.5 of TS 36.331 [15]
Signal-to-noise and interference ratio	OAM (see NOTE 1)	The per UE measurement of the received signal to noise and interference ratio in a network cell, including SS-SINR, CSI-SINR, E-UTRA RS-SINR, as specified in clause 5.1 of TS 38.215 [12]
The mapping information between cell ID and frequency	OAM	The mapping information between cell ID and frequency (NOTE 2).
Cell Energy Saving State	OAM	List of the cells which are within the area of interest and are in energy saving state, as specified in clauses 3.1 and 6.2 of TS 28.310 [24].
NOTE 1: Per UE measurement for a specific UE from OAM (via MDT), is as captured in clause 6.2.3.1. NOTE 2: The MDT measurement report provides the cell identity and carrier frequency information for UE's serving cell and neighbour cell(s). The NWDAF can get the mapping information between cell ID and frequency using OAM service as described in clause 6.2.3.		

NWDAF subscribes the network data from OAM in the Table 6.4.2-3 by using the services provided by OAM as described in clause 6.2.3.

Table 6.4.2-4: UE level Network Data from 5G NF related to the Service Experience

Information	Source	Description
Timestamp	5GC NF	A time stamp associated with the collected information.
Location	AMF	The UE location information, e.g. cell ID or TAI.
UE ID	AMF	(list of)SUPI(s).
RAT Type	SMF	The RAT type the UE camps on.

The Event Filters for the service data collection from SMF, AMF and AF are defined in TS 23.502 [3].

The timestamps are provided by each NF to allow correlation of QoS and traffic KPIs. The clock reference is able to know the accuracy of the time and correlate the time series of the data retrieved from each NF.

6.4.3 Output Analytics

The NWDAF services as defined in the clause 7.2 and 7.3 are used to expose the analytics.

- Service Experience statistics information is defined in Table 6.4.3-1.
- Service Experience predictions information is defined in Table 6.4.3-2.

Table 6.4.3-1: Service Experience statistics

Information	Description
Slice instance service experiences (0..max)	List of observed service experience information for each Network Slice instance.
> S-NSSAI	Identifies the Network Slice
> NSI ID (NOTE 2)	Identifies the Network Slice instance within the Network Slice.
> Network Slice instance service experience	Service experience across Applications on a Network Slice instance over the Analytics target period (average, variance).
> SUPI list (0..SUPImax) (NOTE 3)	List of SUPI(s) for which the slice instance service experience applies.
> Ratio (NOTE 3)	Estimated percentage of UEs with similar service experience (in the group, or among all UEs).
> Spatial validity (NOTE 6)	Area where the Network Slice service experience analytics applies.
> Validity period	Validity period for the Network Slice service experience analytics as defined in clause 6.1.3.
Application service experiences (0..max)	List of observed service experience information for each Application.
> S-NSSAI	Identifies the Network Slice used to access the Application.
> Application ID	Identification of the Application.
> Service Experience Type	Type of Service Experience analytics, e.g. on voice, video, other.
>UE location (NOTE 1, NOTE 5)	Indicating the UE location information (e.g. TAI list, gNB ID, etc) when the UE service is delivered.
>UPF Info (NOTE 4)	Indicating UPF serving the UE.
>DNAI	Indicating which DNAI the UE service uses/camps on.
>DNN (NOTE 4)	DNN for the PDU Session which contains the QoS flow.
>Application Server Instance Address	Identifies the Application Server Instance (IP address of the Application Server) or FQDN of Application Server.
> Service Experience	Service Experience over the Analytics target period (average, variance).
> SUPI list (0..SUPImax) (NOTE 3)	List of SUPI(s) with the same application service experience.
> Ratio (NOTE 3)	Estimated percentage of UEs with similar service experience (in the group, or among all UEs).
> Spatial validity (NOTE 6)	Area where the Application service experience analytics applies.
> Validity period	Validity period for the Application service experience analytics as defined in clause 6.1.3.
> RAT Type (NOTE 7)	Indicating the list of RAT type(s) for which the application service experience analytics applies.
> Frequency (NOTE 7)	Indicating the list of carrier frequency value(s) of UE's serving cell(s) where the application service experience analytics applies.

NOTE 1: This information element is an Analytics subset that can be used in "list of analytics subsets that are requested.

NOTE 2: The NSI ID is an optional parameter. If not provided the Slice instance service experience indicates the service experience for the S-NSSAI.

NOTE 3: The SUPI list and Ratio in the service experience information for an application can be omitted, if the corresponding parameter(s) is/are provided and are assigned with the same value(s) in the service experience information for the slice instance which the application belongs to. Otherwise, the SUPI list and Ratio are mandatory to be provided for an application service experience.

NOTE 4: If the consumer NF is an AF, the item "DNN" and "UPF info" shall not be included, and the NEF is responsible for translation of SUPI to GPSI, internal group identifiers to external ones, and UE location to geographical area, by querying UDM, prior to contacting the AF.

NOTE 5: When possible and applicable to the access type, UE location is provided according to the preferred granularity of location information. UE location shall only be included if the Consumer analytics request is for single UE or a list of UEs. Inclusion of UE location requires user consent.

NOTE 6: The Spatial validity is present in the output parameters if the consumer provided the Area of Interest as defined in Table 6.4.1-1.

NOTE 7: When "any" value has been provided in the request (e.g. "any" RAT type, "any" frequency, or "any" for all the RAT type and frequency indication), the NWDAF provides an instance of the Application service experience per combination of RAT Type(s) and/or Frequency value(s) having the same Service Experience.

Table 6.4.3-2: Service Experience predictions

Information	Description
Slice instance service experiences (0..max)	List of observed service experience information for each Network Slice instance.
> S-NSSAI	Identifies the Network Slice
> NSI ID (NOTE 2)	Identifies the Network Slice instance within the Network Slice.
> Network Slice instance service experience	Service experience across Applications on a Network Slice instance over the Analytics target period (average, variance).
> SUPI list (0..SUPImax) (NOTE 3)	List of SUPI(s) for which the slice instance service experience applies.
> Ratio (NOTE 3)	Estimated percentage of UEs with similar service experience (in the group, or among all UEs).
> Spatial validity (NOTE 6)	Area where the Network Slice service experience analytics applies.
> Validity period	Validity period for the Network Slice service experience analytics as defined in clause 6.1.3.
> Confidence	Confidence of this prediction.
Application service experiences (0..max)	List of predicted service experience information for each Application.
> S-NSSAI	Identifies the Network Slice used to access the Application.
> Application ID	Identification of the Application.
> Service Experience Type	Type of Service Experience analytics, e.g. on voice, video, other.
>UE location (NOTE 1, NOTE 5)	Indicating the UE location information (e.g. TAI list, gNB ID, etc) when the UE service is delivered.
>UPF Info (NOTE 4)	Indicating UPF serving the UE.
>DNAI	Indicating which DNAI the UE service uses/camps on.
>DNN (NOTE 4)	DNN for the PDU Session which contains the QoS flow.
>Application Server Instance Address	Identifies the Application Server Instance (IP address of the Application Server) or FQDN of Application Server.
> Service Experience	Service Experience over the Analytics target period (average, variance).
> SUPI list (0..SUPImax) (NOTE 3)	List of SUPI(s) with the same application service experience.
> Ratio (NOTE 3)	Estimated percentage of UEs with similar service experience (in the group, or among all UEs).
> Spatial validity (NOTE 6)	Area where the Application service experience analytics applies.
> Validity period	Validity period for the Application service experience analytics as defined in clause 6.1.3.
> Confidence	Confidence of this prediction.
> RAT Type (NOTE 7)	Indicating the list of RAT type(s) for which the application service experience analytics applies.
> Frequency (NOTE 7)	Indicating the list of carrier frequency value(s) of UE's serving cell(s) where the application service experience analytics applies.

NOTE 1: This information element is an Analytics subset that can be used in "list of analytics subsets that are requested".
NOTE 2: The NSI ID is an optional parameter. If not provided the Slice instance service experience indicates the service experience for the S-NSSAI.
NOTE 3: The SUPI list and Ratio in the service experience information for an application can be omitted, if the corresponding parameter(s) is/are provided and are assigned with the same value(s) in the service experience information for the slice instance which the application belongs to. Otherwise, the SUPI list and Ratio are mandatory to be provided for an application service experience.
NOTE 4: If the consumer NF is an AF, the item "DNN" and "UPF info" shall not be included, and the NEF is responsible for translation of SUPI to GPSI, internal group identifiers to external ones, and UE location to geographical area, by querying UDM, prior to contacting the AF.
NOTE 5: When possible and applicable to the access type, UE location is provided according to the preferred granularity of location information. UE location shall only be included if the Consumer analytics request is for single UE or a list of UEs. Inclusion of UE location requires user consent.
NOTE 6: The Spatial validity is present in the output parameters if the consumer provided the Area of Interest as defined in Table 6.4.1-1.
NOTE 7: When "any" value has been provided in the request (e.g. "any" RAT type, "any" frequency, or "any" for all the RAT type and frequency indication), the NWDAF provides an instance of the Application service experience per combination of RAT Type(s) and/or Frequency value(s) having the same Service Experience.

The number of Service Experiences and SUPIs are limited respectively by the maximum number of objects and the Maximum number of SUPIs provided as part of Analytics Reporting Information by the NWDAF Service Consumer.

6.4.4 Procedures to request Service Experience for an Application

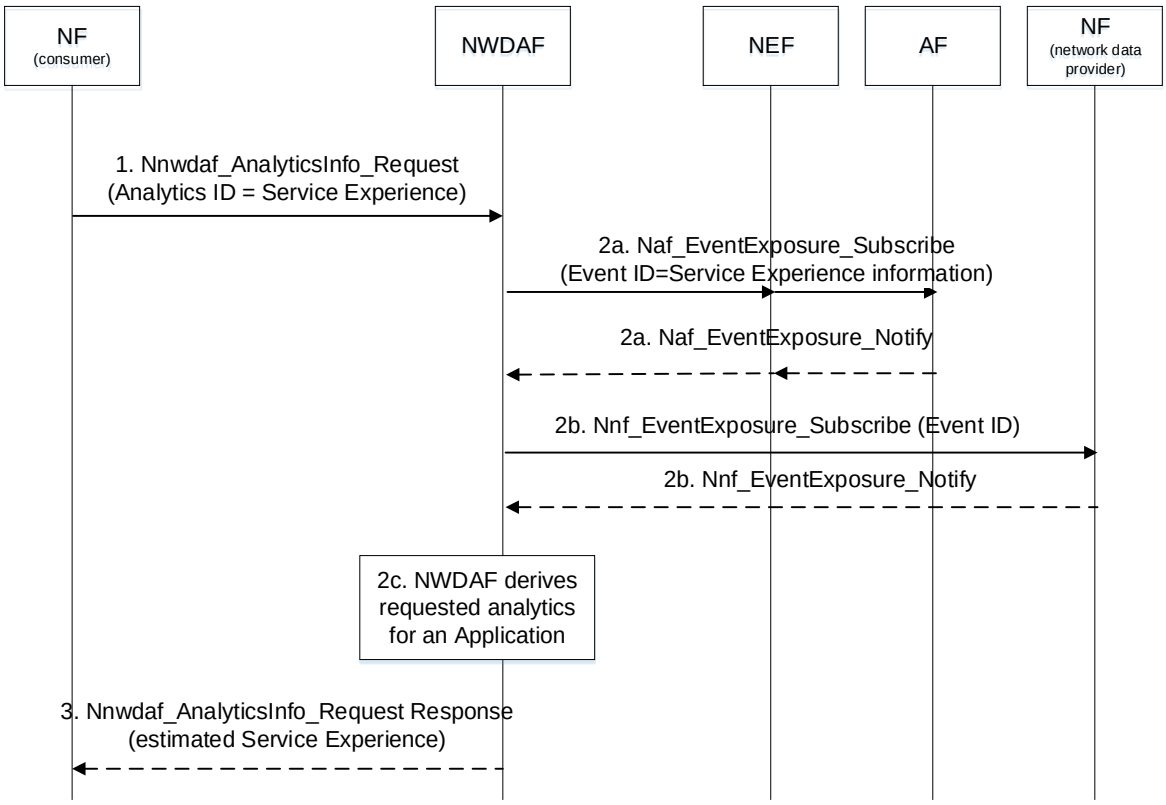

Figure 6.4.4-1: Procedure for NWDAF providing Service Experience for an Application

This procedure allows the consumer to request Analytics ID "Service Experience" for a particular Application. The consumer includes both the Application ID for which the Service Experience is requested and indicates that the Target of Analytics Reporting is "any UE". If the Target for Analytics Reporting is either a SUPI or an Internal-Group-Id the procedure in clause 6.4.6 applies. At the same time, for an Application ID, a set of initial QoS parameter combinations per service experience window (e.g. one is for 3<Service MOS<4 and another is for 4<Service MOS<5) is defined in PCF (e.g. by configuration of operator policies) that may be updated based on the Service Experience reported by NWDAF.

1. Consumer NF sends an Analytics request/subscribe (Analytics ID = Service Experience, Target of Analytics Reporting = any UE, Analytics Filter Information that may include one or more of the following as defined in Table 6.4.1-1 (Application ID, S-NSSAI, DNN, Application Server Address(es), Area of Interest, RAT type(s), Frequency value(s)), Analytics Reporting Information=Analytics target period) to NWDAF by invoking a Nnwdaf_AnalyticsInfo_Request or a Nnwdaf_AnalyticsSubscription_Subscribe.

2a. NWDAF subscribes the service data from AF in the Table 6.4.2-1 by invoking Nnef_EventExposure_Subscribe or Naf_EventExposure_Subscribe service (Event ID = Service Experience information, Application ID, Event Filter information), Target of Event Reporting = Any UE) as defined in TS 23.502 [3].

NOTE 1: In the case of trusted AF, NWDAF provides the Area of Interest as a list of TAIs to AF. In the case of untrusted AF, NEF translates the requested Area of Interest provided as event filter by NWDAF into geographic zone identifier(s) that act as event filter for AF.

2b. NWDAF subscribes the network data from 5GC NF(s) in the Table 6.4.2-2 by invoking Nnf_EventExposure_Subscribe service operation.

2c. With these data, the NWDAF estimates the Service experience for the application.

NOTE 2: QoE measurements from the applications are based on outcome of the ongoing SA5 Rel-16 WID "Management of QoE measurement collection" which addresses how to collect the QoE measurements from the applications in the UE.

3. The NWDAF provides the data analytics, i.e. the observed Service Experience (which can be a range of values) to the consumer NF by means of either Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1, indicating how well the used QoS Parameters satisfy the Service MoS agreed between the MNO and the end user or between the MNO and the external ASP.

NOTE 3: The call flow only shows a request-response model for the interaction of NWDAF and consumer NF for simplicity instead of both request-response model and subscription-notification model.

NOTE 4: The non-real time data information from AF includes the service experience data (see Table 6.4.2-1), which indicates the service quality during the service lifetime.

If the consumer NF is a PCF and it determines that the application SLA is not satisfied, it may take into account the Observed Service Experience and the operator policies including SLA and required Service Experience (which can be a range of values) to determine new QoS parameters to be applied for the service, as defined in clause 6.1.1.3 and clause 6.2.1.2 ofTS 23.503 [4].

If the consumer NF is an AF (e.g. MEC or other Application Server), it may use the Observed Service Experience related network data analytics to determine whether the user experience can be satisfied. If not, the AF may determine to adjust service parameters, e.g. for a video service this may be bit rate, frame rate, codec format, compression parameter, screen size, etc., to better match the network conditions and achieve better user experience.

If the consumer NF is SMF, PCF or AF/Application Server, it may take into account the Observed Service Experience analytics per UP path (i.e. UPF and/or DNAI and/or AS instance address as defined in Table 6.4.3-1) to perform the following procedures:

- The consumer SMF determines to (re)selects UP paths, including UPF and DNAI, as described in clause 4.3.5 ofTS 23.502 [3]. In addition, the SMF may (re)configure traffic steering, updating the UPF regarding the target DNAI with new traffic steering rules.

- The consumer AF/Application Server determines to adjust service parameters, e.g. service parameters of video for adjustment may be bit rate, frame rate, codec format, compression parameter, screen size, etc. In addition, the AF/ Application Server may provide an updated list of DNAI(s) for SMF to perform relocation when appropriate.

- The consumer PCF may provide an updated list of DNAI(s) for SMF to perform relocation upon AF request.

6.4.5 Procedures to request Service Experience for a Network Slice

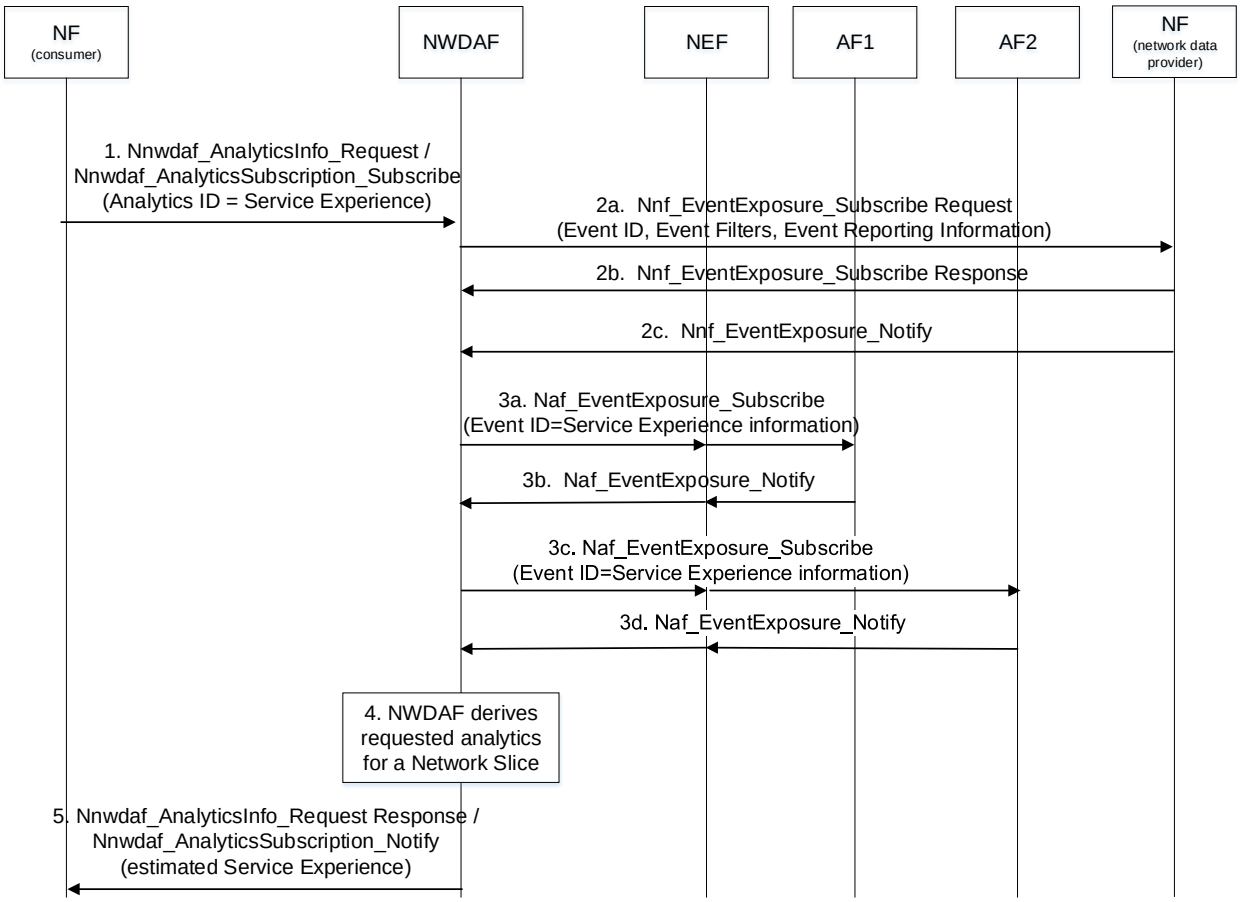

Figure 6.4.5-1: Procedure for NWDAF providing Service Experience for a UE or a group of UEs in a Network Slice

This procedure is similar to the procedure in clause 6.4.4, with the following differences. The consumer needs to request the Analytics ID "Service Experience" for all UEs or a group of UEs or a UE on a Network Slice, identified by an S-NSSAI. If multiple Network Slice instances of the same Network Slice are deployed, associated NSI ID(s) may be used in addition to S-NSSAI. If 'any UE' is the Target of Analytics Reporting, NWDAF may subscribe to UE mobility event notifications of AMF as described in clause 5.3.4.4 of TS 23.501 [2] using event ID "UE moving in or out of Area of Interest" and Event Filters as described in Table 5.2.2.3.1-1 of TS 23.502 [3] if it is needed to retrieve the list of SUPIs (and GPSIs if available) in the area of interest. The event exposure service request may also include the immediate reporting flag as Event Reporting Information as described in Table 4.15.1-1 of TS 23.502 [3].

In addition, service experience data may need to be collected from multiple Applications. If each Application is hosted in different AFs, NWDAF subscribes the service data in the Table 6.4.2-1 from the different AFs by invoking Nnef_EventExposure_Subscribe or Naf_EventExposure_Subscribe services for each Application (Event ID = Service Experience information, Event Filter information, Application ID) as defined in TS 23.502 [3]. Figure 6.4.5-1 shows an example procedure with two AFs. If one AF provides the service experience data of multiple Applications, the set of Application IDs is provided by NWDAF to the AF with the Naf_EventExposure_Subscribe service operation, as defined TS 23.502 [3].

The Observed Service Experience for a Network Slice when consumed by OAM could be used as described in Annex H of TS 28.550 [7].

6.4.6 Procedures to request Service Experience for a UE

Figure 6.4.6-1 depicts procedure for NWDAF providing Service Experience for an application for a UE or a group of UEs.

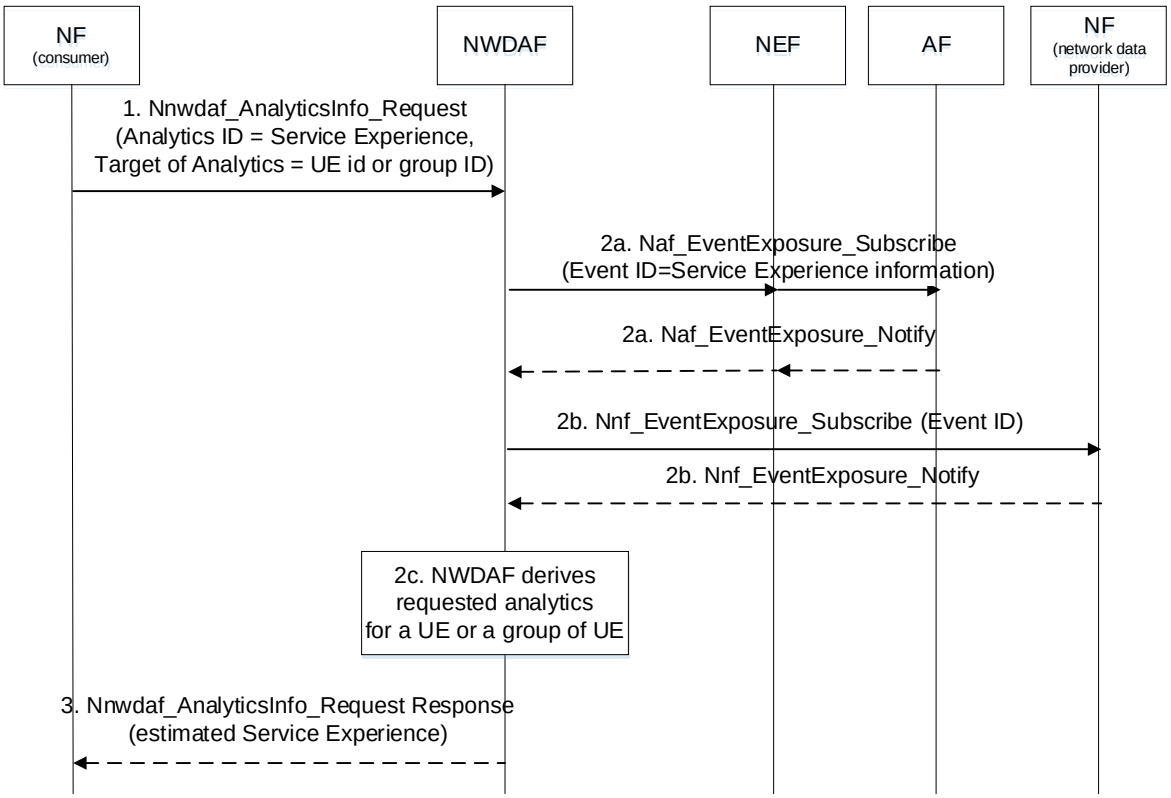

Figure 6.4.6-1: Procedure for NWDAF providing Service Experience for an application for a UE or a group of UEs

The procedure in clause 6.4.4 applies with the following additions. The consumer needs to request the Analytics ID "Service Experience" for a UE identified by a SUPI or a group of UEs identified by an Internal Group-Id. The consumer includes both the Application ID for which their Service Experience is requested and the Target of Analytics Reporting for a SUPI or an Internal-Group-Id. Analytic Filter Information can be set according to clause 6.4.1. When NEF is the NF service consumer, the NEF translates a GPSI into a SUPI or an External-Group-Id into an Internal-Group-Id then includes it in the Target of Analytics Reporting.

6.5 NF load analytics

6.5.1 General

The clause 6.5 describes how NWDAF can provide NF load analytics, in the form of statistics or predictions or both, to another NF.

The service consumer may be an NF, or the OAM.

The consumer of these analytics shall indicate in the request:

- Analytics ID = "NF load information";
- Target of Analytics Reporting: an optional SUPI or any UE;
- Analytics Filter Information:
  - optional S-NSSAI;
  - an optional list of NF Instance IDs, NF Set IDs, or NF types;
  - optional area of interest;
  - an optional list of analytics subsets that are requested (see clause 6.5.3);

- Optional preferred level of accuracy of the analytics;
- Optional preferred level of accuracy per analytics subset (see clause 6.5.3);
- Optional preferred order of results for the list of resource status: ascending or descending NF load;
- Optional Reporting Threshold; the Reporting Threshold is unique for all NFs matching the above Analytics Filter and the reporting applies when the conditions are met for at least one of these NFs;
- An Analytics target period indicates the time period over which the statistics or predictions are requested;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

The NWDAF shall notify the result of the analytics to the consumer as indicated in clause 6.5.3.

If a list of the NF Instance IDs (or respectively of NF Set IDs) is provided, the NWDAF shall provide the analytics for each designated NF instance (or respectively for each NF instance belonging to each designated NF Set). In such case the Target of Analytics Reporting should be ignored.

Otherwise, if a SUPI is provided, the NWDAF shall use the SUPI to determine which NF instances (AMF and SMF) are serving this specific UE, filter them according to the provided S-NSSAI and NF types using data collected from NRF or OAM, and provide analytics for these NF instances.

NOTE: Only NF instances of type AMF and SMF can be determined using a SUPI.

6.5.2 Input data

For the purpose of NF load analytics, the NWDAF may collect the information as listed in Table 6.5.2-1 for the relevant NF instance(s).

Table 6.5.2-1: Data collected by NWDAF for NF load analytics

Information	Source	Description
NF load	NRF	The load of specific NF instance(s) in their NF profile as defined per TS 29.510 [18].
NF status	NRF	The status of a specific NF instance(s) (registered, suspended, undiscoverable) as defined per TS 29.510 [18].
NF resource usage	OAM	The usage of assigned virtual resources currently in use for specific NF instance(s) (mean usage of virtual CPU, memory, disk) as defined in TS 28.552 [8] clause 5.7.
NF resource configuration	OAM	The life cycle changes of specific NF resources (e.g. NF operational or interrupted during virtual/physical resources reconfiguration) as defined in TS 28.533 [19], clause 5.2.

NOTE 1: The OAM information can be used as a complement to NRF information for some or all of the following aspects: resources utilization, NRF information correlation, and alternative source of information if NRF information on load is not available.

NOTE 2: NWDAF can request NRF for data related to NF instances, as described in TS 29.510 [18].

NOTE 3: NWDAF can correlate the NF resources configuration with NF resource usage for generating the analytics output.

If target NF type is UPF, the NWDAF may collect the information as listed in Table 6.5.2-2, in addition to information listed in Table 6.5.2-1.

Table 6.5.2-2: Data collected by NWDAF for UPF load analytics

Information	Source	Description
Traffic usage report	UPF	Report of user plane traffic in the UPF for the accumulated usage of network resources (see TS 29.244 [17])

NOTE 4: How NWDAF collects information in table 6.5.2-2 is not defined in this Release of the specification.

For the purpose of NF load analytics, the NWDAF may collect the information as listed in Table 6.5.2-3 (from OAM via MDT) and Table 6.5.2-5 via the AF (for trusted AF) or NEF (for untrusted AF) in addition to other information described above.

Table 6.5.2-3: MDT input data for UE

Information	Source	Description
UE Speed	OAM (see NOTE 1)	UE Speed (see TS 37.320 [20]).
UE Orientation	OAM (see NOTE 1)	UE Orientation (see TS 37.320 [20]).
NOTE 1: UE input data collection for a specific UE from OAM (via MDT), is as captured in clause 6.2.3.1.		

Table 6.5.2-4: Per UE attribute to be collected and processed by the AF

Information	Source	Description
Per UE attribute	UE Application (see NOTE 1)	UE application data to be collected from UE.
> Destination		Expected final location of UE based on the route planned.
> Route		Planned path of movement by a UE application (e.g. a navigation app). The format is based on the SLA.
> Average Speed		Expected speed over the route planned by a UE application.
> Time of arrival		Expected Time of arrival to destination based on the route planned.
NOTE 1: The procedure for data collection from UE Application is as covered in clause 6.2.8.		

Table 6.5.2-5: AF input data to the NWDAF for Collective Behaviour of UEs

Information	Source	Description
Collective Attribute	AF / NEF (see NOTE 1, NOTE 2)	Characterise collective attribute per set of UEs (see Table 6.5.2-4) within the area of interest.
> Number of UEs		Total number of UEsthat fulfil a collective behaviour within the area of interest.
> Timestamp		A time stamp of time that the collective attribute derived.
> Application ID(s)	(see NOTE 3)	Identifying the application providing this information
> List of UE IDs	(see NOTE 4)	UE IDs that fulfil a collective behaviour within the area of interest.
NOTE 1: For collective behaviour attribute, data processing procedure is as defined in clause 6.2.8. NOTE 2: Per collective attribute, the AF may provide several collective attribute sets, if several sets of UEs with similar behaviour are identified. A similar behaviour can be identified to specific ranges if the AF performs data processing (Data Anonymisation, Aggregation or Normalization) based on NWDAF request. UEs falling in the same range per UE attribute can form a collective attribute set. NOTE 3: The application ID(s) (either external or Internal) is optional. If the application ID(s) is not provided, the relevant application ID(s) can be identified by NWDAF based on the relevant event ID as registered in NRF as covered in clause 6.2.8.2.2. NOTE 4: List of UE IDs is optional and subject to support by the AF when processing the data based on NWDAF request.		

Based on network configuration, NWDAF may discover the AF from the NRF as defined in 6.2.8.2.2 (based on Collective Behaviour as Event ID or a corresponding Application ID).

For AF in trusted domain, the NWDAF invokes step 3a in clause 6.2.8.2.3 by using Naf_EventExposure_Subscribe service (Event ID = Collective Behaviour, Event Filter information, Target of Event Reporting). The collective attribute (see Table 6.5.2-5) can be indicated as part of event filter information as defined in TS 23.502 [3]. Otherwise, the AF notifies for all collective attributes within the area of interest.

For AF in untrusted domain, the NWDAF invokes step 3b in clause 6.2.8.2.3 by using Nnef_EventExposure_Subscribe (Event ID = Collective Behaviour, Event Filter information, Target of Event Reporting). The collective attribute (see Table 6.5.2-5) can be indicated as part of event filter information as defined in TS 23.502 [3]. Otherwise, the AF via NEF notifies for all collective attributes within the area of interest.

For Collective Behaviour of multiple UEs, NWDAF based on the configuration by MNO may request certain type of data processing from the AF as part of event filter information (e.g. for anonymisation, normalisation, aggregation). The data processing requested by NWDAF is used to anonymise, normalise or aggregate the same UE attribute from multiple UEs at the AF before notifying to the NWDAF.

For each UE attribute of a specific UE, whether and how AF is processing the data that is received from the UE depends on the SLA configured in AF (defined in clause 6.2.8.1) and is not known by the NWDAF.

To determine NF load (per area of interest), NWDAF may collect and take into account UE trajectory input data from the AF, defined in clause 6.7.2.2, Table 6.7.2.2-2 for UE mobility analytics in addition to MDT input data and /or collective behaviour input data, defined in clause 6.5.2, Table 6.5.2-3 and Table 6.5.2-5, respectively.

6.5.3 Output analytics

The NWDAF services as defined in the clause 7.2 and 7.3 are used to expose the analytics. NF load statistics information are defined in Table 6.5.3-1. NF load predictions information are defined in Table 6.5.3-2.

Table 6.5.3-1: NF load statistics

Information	Description
List of resource status (1..max)	List of observed load information for each NF instance along with the corresponding NF id / NF Set ID (as applicable).
> NF type	Type of the NF instance.
> NF instance ID	Identification of the NF instance.
> NF status (NOTE 1)	The availability status of the NF on the Analytics target period, expressed as a percentage of time per status value (registered, suspended, undiscoverable).
> NF resource usage (NOTE 1)	The average usage of assigned resources (CPU, memory, disk).
> NF load (NOTE 1)	The average load of the NF instance over the Analytics target period.
> NF peak load (NOTE 1)	The maximum load of the NF instance over the Analytics target period.
> NF load (per area of interest)(NOTE 2)	The average load of the NF instances over the area of interest.
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested" and "Preferred level of accuracy per analytics subset". NOTE 2: Applicable only to AMF load based on Input data in clause 6.5.2, Table 6.5.2-3 and Table 6.5.2-5.	

Table 6.5.3-2: NF load predictions

Information	Description
List of resource status (1..max)	List of predicted load information for each NF instance along with the corresponding NF id / NF Set ID (as applicable)
> NF type	Type of the NF instance
> NF instance ID	Identification of the NF instance
> NF status (NOTE 1)	The availability status of the NF on the Analytics target period, expressed as a percentage of time per status value (registered, suspended, undiscoverable)
> NF resource usage (NOTE 1)	The average usage of assigned resources (CPU, memory, disk)
> NF load (NOTE 1)	The average load of the NF instance over the Analytics target period
> NF peak load (NOTE 1)	The maximum load of the NF instance over the Analytics target period
> Confidence	Confidence of this prediction
> NF load (per area of interest) (NOTE 2)	The predicted average load of the NF instances over the area of interest.
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested" and "Preferred level of accuracy per analytics subset". NOTE 2: Applicable only to AMF load based on Input data in clause 6.5.2, Table 6.5.2-3 and Table 6.5.2-5.	

NOTE: The variations on per-instance NF load and resource usage could be influenced by the number of running NF instances in addition to the load itself.

The predictions are provided with a Validity Period, as defined in clause 6.1.3.

The number of resource status is limited by the maximum number of objects provided as part of Analytics Reporting Information.

6.5.4 Procedures

The procedure depicted in Figure 6.5.4-1 allows a consumer NF to request analytics to NWDAF for NF load of various NF instances as defined in 6.5.1.

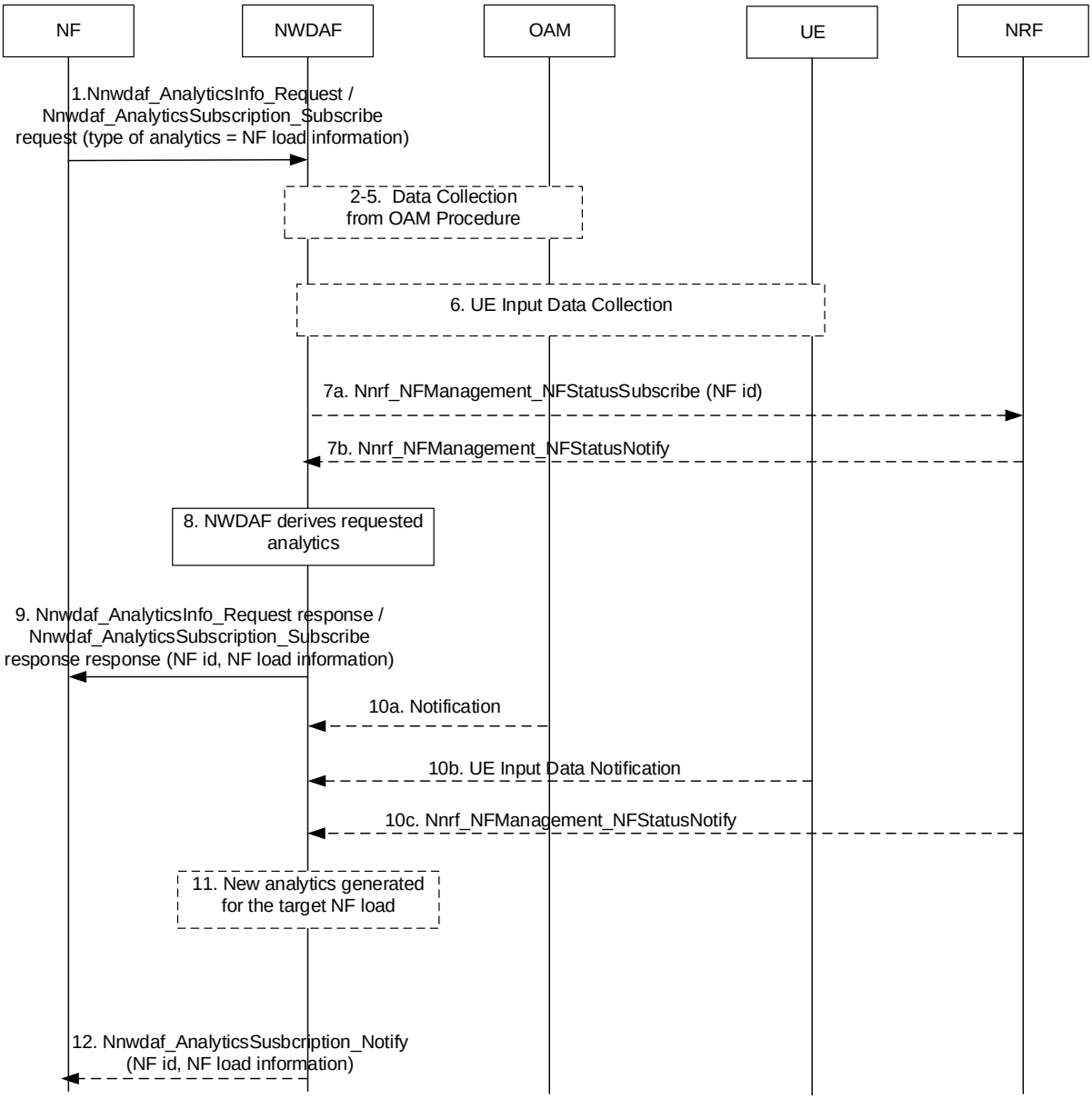

Figure 6.5.4-1: NF load analytics provided by NWDAF

1. The NF sends a request to the NWDAF for analytics for NF load for a specific NF, using either the Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription service. The Analytics ID is set to NF load information, the Target of Analytics Reporting and the Analytics Filter Information are set according to clause 6.5.1. The NF can request statistics or predictions or both and can provide a time window.

2-5. If the request is authorized, and in order to provide the requested analytics, the NWDAF may need for each NF targeted instance to subscribe to OAM services to retrieve the target NF resource usage and NF resources configuration following steps captured in clause 6.2.3.2 for data collection from OAM. The NWDAF may collect MDT input data per individual UE from OAM (see Table 6.5.2-3). Steps 2-5 may be skipped when e.g. the NWDAF already has the requested analytics.

6. For Collective Behaviour attributes, if the request is authorized, and in order to provide the requested analytics, NWDAF may follow the UE Input Data Collection Procedure via the AF as defined in clause 6.2.8 (see Table 6.5.2-4 and Table 6.5.2-5).

   The NWDAF subscribes to the AF services as above invoking either Nnef_EventExposure_Subscribe or Naf_EventExposure_Subscribe service (Event ID = Collective Behaviour, Event Filter information, Target of Event Reporting) as defined in TS 23.502 [3]. The area of interest is set as part of Event Filter information to specific TAs or AMF region. The UE data is collected from UEs within the area of interest.

In the case of trusted AF, the NWDAF provides the Area of Interest as a list of TAIs to the AF. In the case of untrusted AF, NEF translates the requested Area of Interest provided as event filter by the NWDAF into geographic zone identifier(s) that act as event filter for the AF.

For collective attributes as defined in Table 6.5.2-5, the AF processes (e.g. anonymize, aggregate and normalize) the data from individual UEs per UE attribute (see Table 6.5.2-4) based on Event Filters indicated by the NWDAF to determine which ones display a collective behaviour within the area of interest before notifying a collective attribute directly (trusted AF) or via NEF (for untrusted AF) to the NWDAF. The AF will provide (per collective attribute) e.g. the number of UEs that fulfil the collective attribute (within an area of interest).

NOTE 1: The call flow only shows a subscription/notification model for the simplicity, however both request-response and subscription-notification models should be supported.

NOTE 2: If the target NF type is UPF, the NWDAF can collect the information as listed in Table 6.5.2-2. How the NWDAF collects information is not defined in this Release of the specification.

7a. The NWDAF subscribes to changes on the load and status of NF instances registered in NRF and identified by their NF id from NRF using Nnrf_NFManagement_NFStatusSubscribe service operation for each NF instance.

7b. NRF notifies NWDAF of changes on the load and status of the requested NF instances by using Nnrf_NFManagement_NFStatusNotify service operation.

8. The NWDAF derives requested analytics.

9. The NWDAF provide requested NF load analytics to the NF along with the corresponding Validity Period or area of interest, using either the Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Subscribe response, depending on the service used in step 1.

10-12. If at step 1 the NF has subscribed to receive continuous reporting of NF load analytics, the NWDAF may generate new analytics and, when relevant according to the Analytics target period and Reporting Threshold, provide them along with the corresponding Validity Period to the NF upon reception of notification of new NF load information from OAM or NRF or UE Input data notification via MDT or the AF (see Table 6.5.2-3 and Table 6.5.2-5).

NOTE 3: If the target NF type at step 1 is UPF, the NWDAF can generate new analytics when receiving new information as listed in Table 6.5.2-2. How the NWDAF receives such new information is not defined in this Release of the specification.

6.6 Network Performance Analytics

6.6.1 General

With Network Performance Analytics, NWDAF provides either statistics or predictions on the gNB status information, gNB resource usage, communication performance and mobility performance in an Area of Interest; in addition, NWDAF it may provide statistics or predictions on the number of UEs that are located in that Area of Interest.

The service consumer may be an NF (e.g. PCF, NEF, AF), or the OAM.

The consumer of these analytics may indicate in the request:

- Analytics ID = "Network Performance";
- Target of Analytics Reporting: either a single UE (SUPI), or a group of UEs (an Internal Group ID that refers to the group for which the analytics on the number of UEs that are located in the Area of Interest at the time indicated in the Analytics target period is requested) or any UE;
- Analytics Filter Information:
  - Area of Interest (list of TA or Cells) which restricts the area in focus (mandatory if Target of Analytics Reporting is set to "any UE", optional otherwise);
  - Optionally, a list of analytics subsets that are requested among those specified in clause 6.6.3;
- Optionally, a preferred level of accuracy of the analytics;

- Optionally, preferred level of accuracy per analytics subset (see clause 6.6.3);
- Optionally, preferred order of results for the list of Network Performance information:
  - ordering criterion: "number of UEs", "communication performance" or "mobility performance";
  - order: ascending or descending;
- Optionally, Reporting Thresholds, which apply only for subscriptions and indicate conditions on the level to be reached for respective analytics information (see clause 6.6.3) in order to be notified by the NWDAF;
- An Analytics target period indicates the time period over which the statistics or prediction are requested; and
- Optionally, maximum number of objects.
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

The NWDAF notifies the result of the analytics to the consumer as indicated in clause 6.6.3.

6.6.2 Input Data

The NWDAF collects Load and Performance information in an Area of Interest from the sources listed in Table 6.6.2-1 and number of UEs within Area of Interest from the sources listed in Table 6.6.2-2.

Table 6.6.2-1: Load and Performance information collected by NWDAF

Load information	Source	Description
Status, load and performance information	OAM	Statistics on RAN status (up/down), load (i.e. Radio Resource Utilization) and performance per Cell Id in the Area of Interest as defined in TS 28.552 [8].
NF Load information	NRF	Load per NF

Table 6.6.2-2: Number of UEs in Area of Interest information collected by NWDAF

Number of UEs information	Source	Description
Number of UEs	AMF	Number of UEs in an Area of Interest

The NWDAF shall be able to collect UE mobility information as stated in clause 6.7.2.2.

6.6.3 Output Analytics

The NWDAF shall be able to provide both statistics and predictions on Network Performance.

Network performance statistics are defined in Table 6.6.3-1.

Table 6.6.3-1: Network performance statistics

Information	Description
List of network performance information (1..max)	Observed statistics during the Analytics target period
> Area subset	TA or Cell ID within the requested area of interest as defined in clause 6.6.1
> Analytics target period subset	Time window within the requested Analytics target period as defined in clause 6.6.1.
> gNB status information (NOTE 1)	Average ratio of gNBs that have been up and running during the entire Analytics target period in the area subset
> gNB resource usage (NOTE 1)	Average usage of assigned resources (CPU, memory, disk)
> Number of UEs (NOTE 1)	Average number of UEs observed in the area subset
> Communication performance (NOTE 1)	Average ratio of successful setup of PDU Sessions
> Mobility performance (NOTE 1)	Average ratio of successful handover
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested" and "Preferred level of accuracy per analytics subset".	

Network performance predictions are defined in Table 6.6.3-2.

Table 6.6.3-2: Network performance predictions

Information	Description
List of network performance information (1..max)	Predicted analytics during the Analytics target period
> Area subset	TA or Cell ID within the requested area of interest as defined in clause 6.6.1
> Analytics target period subset	Time window within the requested Analytics target period as defined in clause 6.6.1.
> gNB status information (NOTE 1)	Average ratio of gNBs that will be up and running during the entire Analytics target period in the area subset
> gNB resource usage (NOTE 1)	Average usage of assigned resources (CPU, memory, disk) (average, peak)
> Number of UEs (NOTE 1)	Average number of UEs predicted in the area subset
> Communication performance (NOTE 1)	Average ratio of successful setup of PDU Sessions
> Mobility performance (NOTE 1)	Average ratio of successful handover
> Confidence	Confidence of this prediction
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested" and "Preferred level of accuracy per analytics subset".	

NOTE 1: The predictions are provided with a Validity Period, as defined in clause 6.1.3.

NOTE 2: The analytics on number of UEs are related to the information retrieved from the AMFs.

The number of network performance information entries is limited by the maximum number of objects provided as part of Analytics Reporting Information.

The NWDAF provides Network Performance Analytics to a consumer at the time requested by the consumer in the Analytics target period:

- Analytics ID set to "Network Performance".
- Notification Target Address including the address of the consumer.
- Notification Correlation Id, for the consumer to correlate notifications from NWDAF if subscription applies.
- Analytics specific parameters at the time indicated in the Analytics target period.

6.6.4 Procedures

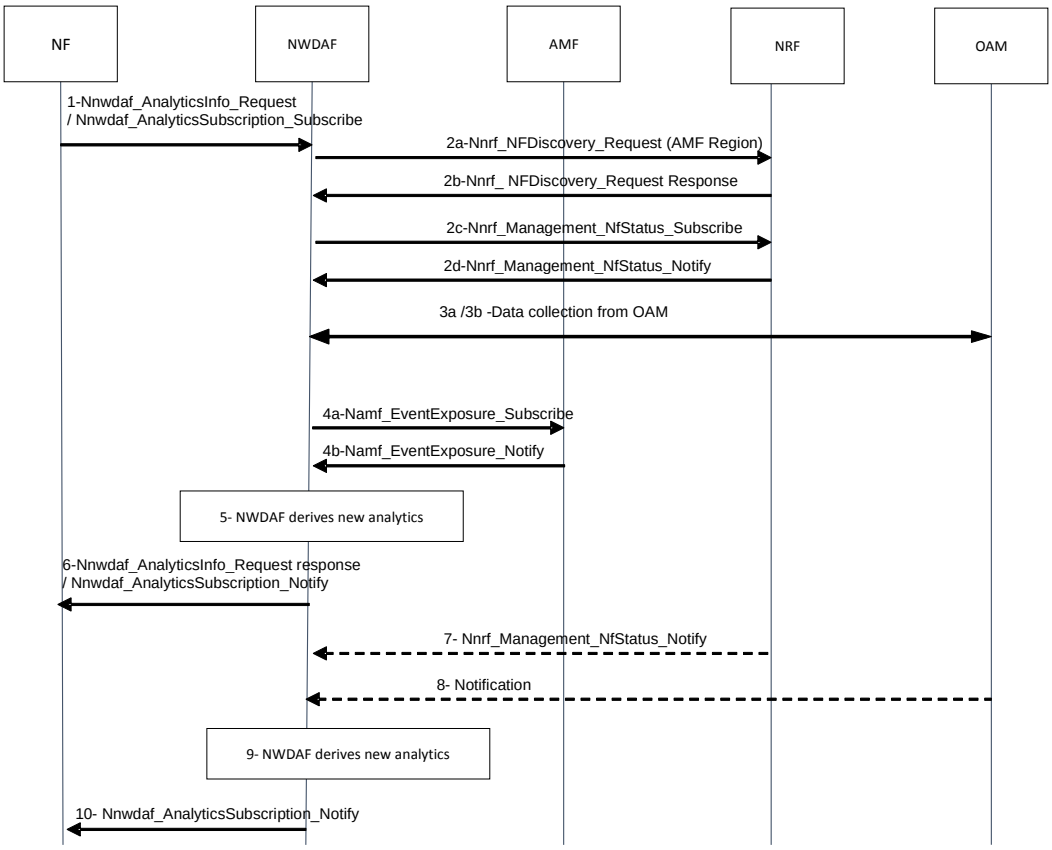

Figure 6.6.4-1: Procedure for subscription to network performance analytics

1. The NF sends Nnwdaf_AnalyticsSubscription_Subscribe or Nnwdaf_AnalyticsInfo_Request (Analytics ID="Network Performance", Target of Analytics Reporting, Analytics Filter Information ="Area of Interest", Analytics Reporting Information=("Reporting Thresholds" and Analytics target Period(s))) to the NWDAF.

2a-2d. The NWDAF discovers from NRF the AMF(s) belonging to the AMF Region(s) that include(s) the Area of Interest and subscribes to NF load and status information from NRF about these AMF(s).

3a-3b. The NWDAF subscribes to OAM services to get the status and load information and the resource usage on the Area of Interest in clause 6.6.2, following the procedure captured in Clause 6.2.3.2.

4a-4b. The NWDAF collects the number of UEs located in the Area of Interest from AMF using Namf_EventExposure_Subscribe service, including the Target of Event Reporting provided as an input parameter (i.e. any UE or Internal Group Identifier).

5. The NWDAF derives the requested analytics.

6. The NWDAF sends Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response (Network Performance analytics, Subscription Correlation Id, Confidence).

7-8. A change of network performance information, i.e. change in the gNB status information, gNB resource usage, communication performance and mobility performance in the area of interest at the observed period, is detected by OAM, or a change in the NF load information is reported by NRF, and is notified to NWDAF.

9. The NWDAF derives new analytics taking into account the most recent data collected.

10. When relevant according to the Analytics target period and Reporting Thresholds, the NWDAF provides a notification using Nnwdaf_AnalyticsSubscription_Notify (Network Performance analytics, Subscription Correlation Id, Confidence).

6.7 UE related analytics

6.7.1 General

This clause specifies the UE related analytics which can be provided by NWDAF:

- UE mobility analytics;
- UE communication analytics;
- Expected UE behavioural parameters related network data analytics; and
- Abnormal behaviour related network data analytics.

The NWDAF service consumer may request for these analytics separately, or in a combined way. As an example, an NWDAF service consumer may learn from the NWDAF the expected UE behaviour parameters as defined in clause 4.15.6.3 ofTS 23.502 [3] for a group of UEs or a specific UE, by requesting analytics for both UE mobility (see clause 6.7.2) and for UE communication (see clause 6.7.3).

Depending on local regulations, the NWDAF retrieves user consent for the UE with UDM prior to data collection as defined in clause 6.2.2.2 or clause 6.2.2.3. If user consent to collect data is not granted by the UE, the NWDAF rejects/cancels any analytics subscriptions to any of the UE related analytics with target for analytics set to the SUPI or GPSI of that UE. If the target for analytics is either an Internal or External Group Id or a list of SUPIs or "any UE", the NWDAF skips those SUPIs that do not grant user consent for the purpose of analytics or model training.

NOTE: Possible uses of such analytics is for the AMF to learn about expected UE behaviour to derive appropriate MICO mode configuration, or for an AF to learn about expected UE behaviour to further provision 5GC with appropriate UE parameters.

6.7.2 UE mobility analytics

6.7.2.1 General

NWDAF supporting UE mobility statistics or predictions shall be able to collect UE mobility related information from NF, OAM, and to perform data analytics to provide UE mobility statistics or predictions.

The service consumer may be a NF (e.g. AMF, SMF or AF).

The consumer of these analytics may indicate in the request:

- Analytics ID = "UE Mobility".
- Target of Analytics Reporting: a single UE (SUPI) or a group of UEs (an Internal Group ID);
- Analytics Filter Information optionally containing:
  - Area of Interest (AOI): restricts the scope of the UE mobility analytics to the provided area;
  - Visited Area(s) of Interest (visited AOI(s)): additional filter to only consider UEs that are currently (i.e. now) in the "AOI" and had previously (i.e. in the "Analytics target period") been in at least one of the Visited AOI(s). If this parameter is provided, the Analytics target period shall be in the past (i.e. supported for statistics only);

NOTE 1: For LADN service, the consumer (e.g. SMF) provides the LADN DNN to refer the LADN service area as the AOI.

- An Analytics target period indicates the time period over which the statistics or predictions are requested;

NOTE 2: For regular analytics scenarios, the Analytics target period is associated with the Analytics Filter Information=AOI, while for the scenario that Analytics ID=UE Mobility and Analytics Filter Information=(AOI and visited AOI(s)), as described in this clause, the Analytics target period is associated with the visited AOI(s) and to obtain the statistics for those UEs that currently reside in the AOI and had previously (i.e. in the "Analytics target period") been in at least one of the Visited AOI(s).

- Optionally, maximum number of objects;
- Preferred level of accuracy of the analytics;
- Preferred order of results for the time slot entries: ascending or descending time slot start;
- Optionally, preferred granularity of location information: TA level or cell level; and
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

6.7.2.2 Input Data

The NWDAF supporting data analytics on UE mobility shall be able to collect UE mobility information from OAM, 5GC and AFs. The detailed information collected by the NWDAF could be MDT data from OAM, network data from 5GC and/or service data from AFs:

- UE mobility information from OAM is UE location carried in MDT data;
- Network data related to UE mobility from 5GC is UE location information, UE location trends or UE access behaviour trends, as defined in the Table 6.7.2.2-1;

Table 6.7.2.2-1: UE Mobility information collected from 5GC

Information	Source	Description
UE ID	AMF	SUPI
UE locations (1..max)	AMF	UE positions
>UE location		TA or cells that the UE enters (NOTE)
>Timestamp		A time stamp when the AMF detects the UE enters this location
Type Allocation code (TAC)	AMF	To indicate the terminal model and vendor information of the UE. The UEs with the same TAC may have similar mobility behaviour. The UE whose mobility behaviour is unlike other UEs with the same TAC may be an abnormal one.
Frequent Mobility Registration Update	AMF	A UE (e.g. a stationary UE) may re-select between neighbour cells due to radio coverage fluctuations. This may lead to multiple Mobility Registration Updates if the cells belong to different registration areas. The number of Mobility Registration Updates N within a period M may be an indication for abnormal ping-pong behaviour, where N and M are operator's configurable parameters.
UE access behaviour trends	AMF	Metrics on UE state transitions (e.g., access, RM and CM states, handover).
UE location trends	AMF	Metrics on UE locations.
NOTE: UE location includes either the last known location or the current location, under the conditions defined in Table 4.15.3.1-1 in TS 23.502 [3].		

- Service data related to UE mobility provided by AFs is defined in the Table 6.7.2.2-2;

Table 6.7.2.2-2: Service Data from AF related to UE mobility

Information	Description
UE ID	Could be external UE ID (i.e. GPSI)
Application ID	Identifying the application providing this information
UE trajectory (1..max)	Timestamped UE positions
>UE location	Geographical area that the UE enters
>Timestamp	A time stamp when UE enters this area
NOTE: The application ID is optional. If the application ID is omitted, the collected UE mobility information can be applicable to all the applications for the UE.	

Depending on the requested level of accuracy, data collection may be provided on samples (e.g. spatial subsets of UEs or UE group, temporal subsets of UE location information).

NOTE: Reporting current UE location can cause AMF to request NG-RAN to report UE location and consequently extra signalling and load in NG-RAN and AMF. The consumer retrieving data from AMF needs to use current location with care to avoid excessive signalling.

6.7.2.3 Output Analytics

The NWDAF supporting data analytics on UE mobility shall be able to provide UE mobility analytics to consumer NFs or AFs. The analytics resultsprovided by the NWDAF could be UE mobility statistics as defined in table 6.7.2.3-1, UE mobility predictions as defined in Table 6.7.2.3-2:

Table 6.7.2.3-1: UE mobility statistics

Information	Description
UE group ID or UE ID	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, SUPI (see NOTE 1).
Time slot entry (1..max)	List of time slots during the Analytics target period
> Time slot start	Time slot start within the Analytics target period
> Duration	Duration of the time slot
> UE location (1..max)	Observed location statistics (see NOTE 2)
>> UE location	TA or cells which the UE stays (see NOTE 3)
>> Ratio	Percentage of UEs in the group (in the case of a UE group)

Table 6.7.2.3-2: UE mobility predictions

Information	Description
UE group ID or UE ID	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or SUPI (see NOTE).
Time slot entry (1..max)	List of predicted time slots
>Time slot start	Time slot start time within the Analytics target period
> Duration	Duration of the time slot
> UE location (1..max)	Predicted location prediction during the Analytics target period
>> UE location	TA or cells where the UE or UE group may move into (see NOTE 3)
>> Confidence	Confidence of this prediction
>> Ratio	Percentage of UEs in the group (in the case of a UE group)

NOTE: When Target of Analytics Reporting is an individual UE, one UE ID (i.e. SUPI) will be included, the NWDAF will provide the analytics mobility result (i.e. list of (predicted) time slots) to NF service consumer(s) for the UE.

NOTE 2: If Visited AOI(s) was provided in the analytics request/subscription, the UE location provides information on the observed location(s) that the UE or group of UEs had been residing during the Analytics Target Period.

NOTE 3: When possible and applicable to the access type, UE location is provided according to the preferred granularity of location information.

The results for UE groups address the group globally. The ratio is the proportion of UEs in the group at a given location at a given time.

The number of time slots and UE locations is limited by the maximum number of objects provided as part of Analytics Reporting Information

The time slots shall be provided by order of time, possibly overlapping. The locations shall be provided by decreasing value of ratio for a given time slot. The sum of all ratios on a given time slot must be equal or less than 100%. Depending on the list size limitation, the least probable locations on a given Analytics target period may not be provided.

6.7.2.4 Procedures

The NWDAF can provide UE mobility related analytics, in the form of statistics or predictions or both, directly to another NF. If the NF is an AF, and when the AF is untrusted, the AF will request analytics via the NEF, and the NEF will then convey the request to NWDAF.

NOTE: In the case of untrusted AF the Target of Analytics Reporting can be a GPSI or an External Group Identifier that is mapped in the 5GC to a SUPI or an Internal Group Identifier.

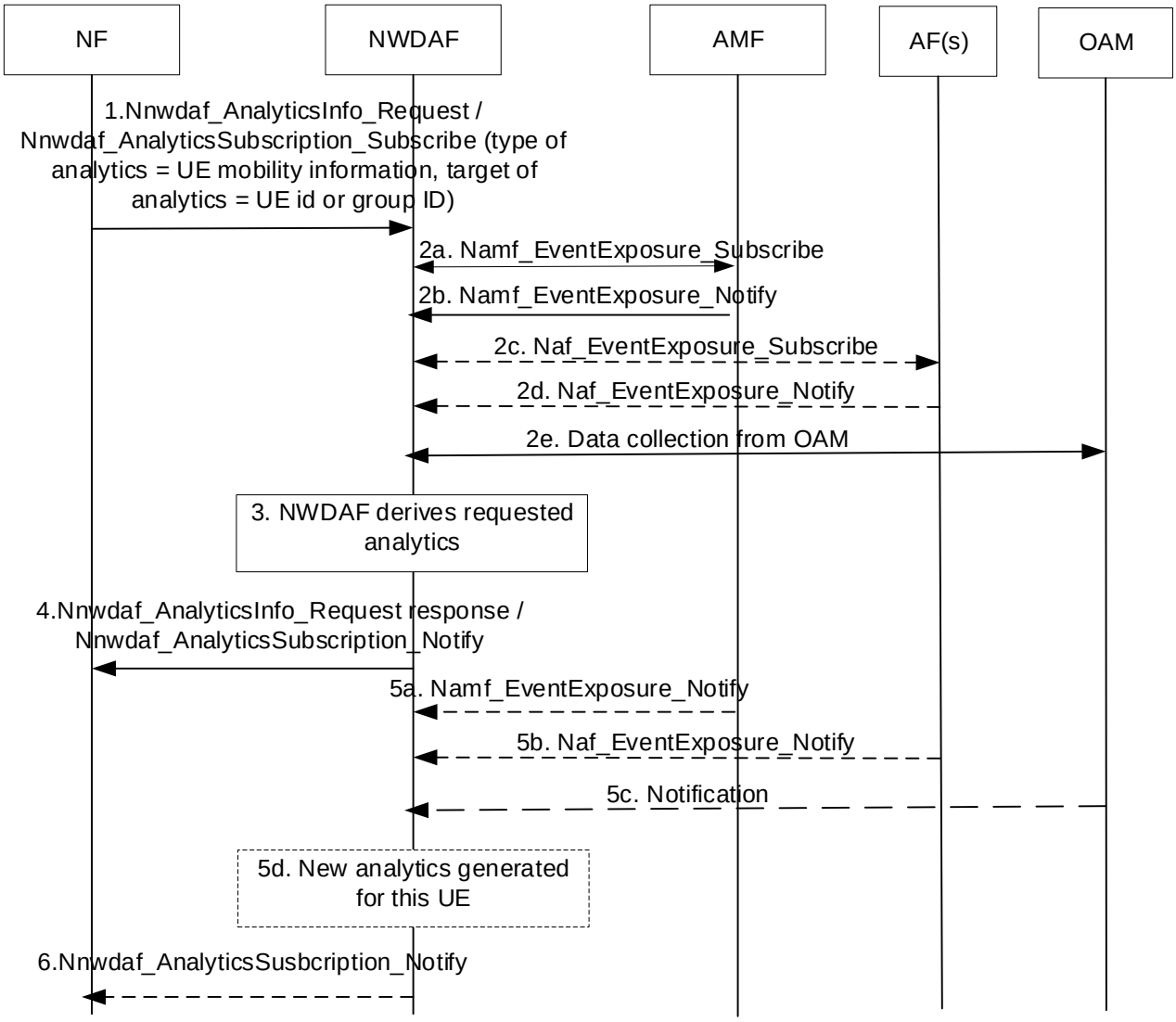

Figure 6.7.2.4-1: UE mobility analytics provided to an NF

1. The NF sends a request (Analytics ID = UE mobility, Target of Analytics Reporting = UE id or Internal Group ID, Analytics Filter Information =AOI, Analytics Reporting Information= Analytics target period) to the serving NWDAF for analytics information on a specific UE or a group of UEs, using either the Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription service to derive UE mobility information. The NF can request statistics or predictions or both. For LADN service, the NF (i.e. SMF) provides LADN DNN as AOI in the Analytics Filter Information.

   If NF wants to obtain the aggregated mobility analytics of those UEs, that currently reside in the AOI and had visited at least one of visited AOI(s) during an Analytics target period, the NF may send a request for UE mobility analytics with Analytics ID = UE mobility, Target of Analytics Reporting = UE group ID or UE ID, Analytics Filter Information = (AOI, visited AOI(s)), Analytics Reporting information = Analytics target period. In this case, the requested mobility analytics is a statistics.

2. If the request is authorized, and in order to provide the requested analytics, the NWDAF may subscribe to events with all the serving AMFs for the requested UE(s), for notification of location changes. This step may be skipped when e.g. the NWDAF already has the requested analytics available.

   The NWDAF subscribes the service data for the requested UE(s) from AF(s) in the Table 6.7.2.2-2 by invoking Naf_EventExposure_Subscribe service or Nnef_EventExposure_Subscribe (if via NEF) using event ID "UE Mobility information" as defined in TS 23.502 [3].

The NWDAF collects UE mobility information from OAM for the requested UE(s), following the procedure captured in clause 6.2.3.2.

NOTE 1: The NWDAF determines the AMF serving the UE or the group of UEs as described in clause 6.2.2.1.

3. The NWDAF derives requested analytics.

   If in step 1 the NWDAF receives analytics subscription/request from NF to obtain the aggregated mobility analytics of those UEs, which currently reside in AOI and had visited at least one of visited AOI(s) during an Analytics target period and if visited AOI(s) and AOI are covered by different NWDAFs, in addition to the data collected in the AOI in step 2, the NWDAF can also obtain UE mobility analytics in one of the visited AOI(s) during the Analytics target period from other NWDAF instance(s) for the requested UE(s). Then the NWDAF supporting analytics aggregation capability derives a UE ID list based on the request from the NF in step 1 and the requested aggregated analytics based on the data collected in the AOI in step 2 and UE mobility analytics in one or more of the visited AOI(s) obtained from the other NWDAF instance(s). UE visited locations in visited AOI(s) and AOI will be included in the aggregated UE mobility analytics.

NOTE 2: If the visited AOI(s) and AOI are covered by different NWDAFs, then consumer in the AOI firstly discovers a NWDAF supporting analytics aggregation capability in the AOI from the NRF, as defined in clause 6.3.13 ofTS 23.501 [2].

4. The NWDAF provides requested UE mobility analytics to the NF, using either the Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1. The details for UE mobility analytics provided by NWDAF are defined in clause 6.7.2.3.

   If in step 1 the NF wants to obtain the aggregated mobility analytics of those UEs, that currently reside in the AOI and had visited at least one of visited AOI(s) during an Analytics target period, the NWDAF will provide the requested aggregated analytics for the UE(s) matching this criteria, i.e. the derived mobility analytics can cover a subset of UEs compared to the Target of Analytics Reporting as provided in step 1.

5-6. If at step 1, the NF has subscribed to receive notifications for UE mobility analytics, after receiving event notification from the AMFs, AFs and OAM subscribed by NWDAF in step 2, the NWDAF may generate new analytics and provide them to the NF.

6.7.3 UE Communication Analytics

6.7.3.1 General

In order to support some optimized operations, e.g. customized mobility management, traffic routing handling, RFSP Index Management, QoS improvement or Inactivity Timer optimization, in 5GS, an NWDAF may perform data analytics on UE communication pattern and user plane traffic, and provide the analytics results (i.e. UE communication statistics or prediction) to NFs in the 5GC.

An NWDAF supporting UE Communication Analytics collects per-application communication description from AFs. If consumer NF provides an Application ID, the NWDAF only considers the data from AF, SMF and UPF that corresponds to this application ID. NWDAF may also collect data from AMF.

The consumer of these analytics may indicate in the request:

- Analytics ID = "UE Communication".
- Target of Analytics Reporting: a single UE (SUPI) or a group of UEs (an Internal Group ID).
- Analytics Filter Information optionally including:
  - S-NSSAI;
  - DNN;
  - Application ID;
  - Area of Interest.
  - an optional list of analytics subsets that are requested (see clause 6.7.3.3);

- An Analytics target period indicates the time period over which the statistics or predictions are requested.
- Preferred level of accuracy of the analytics.
- Optional Preferred level of accuracy per analytics subset (see clause 6.7.3.3);
- Optional preferred order of results for the list of UE Communications:
  - ordering criterion: "start time" or "duration",
  - order: ascending or descending;
- Optionally, maximum number of objects;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

6.7.3.2 Input Data

The NWDAF supporting data analytics on UE communication shall be able to collect communication information for the UE from 5GC. The detailed information collected by the NWDAF includes service data related to UE communication as defined in the Table 6.7.3.2-1.

Table 6.7.3.2-1: Service Data from 5GC related to UE communication

Information	Source	Description
UE ID	SMF, AF	SUPI in the case of SMF, external UE ID (i.e. GPSI) in the case of AF
Group ID	SMF, AF	To identify UE group if available Internal Group ID in the case of SMF, External Group ID in the case of AF
S-NSSAI	SMF	Information to identify a Network Slice
DNN	SMF	Data Network Name where PDU connectivity service is provided
Application ID	SMF, AF	Identifying the application providing this information
Expected UE Behaviour parameters	AF	Same as Expected UE Behaviour parameters specified in TS 23.502 [3]
UE communication (1..max)	UPF, AF	Communication description per application
>Communication start		The time stamp that this communication starts
>Communication stop		The time stamp that this communication stops
>UL data rate		UL data rate of this communication
>DL data rate		DL data rate of this communication
>Traffic volume		Traffic volume of this communication
Type Allocation code (TAC)	AMF	To indicate the terminal model and vendor information of the UE. The UEs with the same TAC may have similar communication behaviour. The UE whose communication behaviour is unlike other UEs with the same TAC may be an abnormal one.
UE locations (1..max)	AMF	UE positions
>UE location		TA or cells that the UE enters
>Timestamp		A time stamp when the AMF detects the UE enters this location
UE location trends	AMF	Metrics on UE locations.
PDU Session ID (1..max)	SMF	Identification of PDU Session.
> N4 Session ID	SMF, UPF	Identification of N4 Session.
> Inactivity detection time	SMF, UPF	Value of session inactivity timer.
> PDU Session status	SMF	Status of the PDU Session (activated, deactivated).
UE CM state	AMF	UE connection management state (e.g. CM-IDLE).
UE session behaviour trends	SMF	Metrics on UE state transitions (e.g. "PDU Session Establishment", "PDU Session Release").
UE communication trends	SMF	Metrics on UE communications.
UE access behaviour trends	AMF	Metrics on UE state transitions (e.g., access, RM and CM states, handover).

NOTE 1: How NWDAF collects UE communication related data from UPF is not defined in this Release of the specification.

NOTE 2: SMF collects N4 Session Level data from UPF independently of NWDAF input data requests to SMF.

Depending on the requested level of accuracy, data collection may be provided on samples (e.g. spatial subsets of UEs or UE group, temporal subsets of UE communication information).

The application Id is optional. If the application Id is omitted, the collected UE communication information can be applicable to all the applications for the UE.

6.7.3.3 Output Analytics

The NWDAF supporting UE Communication Analytics provides the analytics results to consumer NFs. The analytics resultsprovided by the NWDAF include the UE communication statistics as defined in Table 6.7.3.3-1 or predictions as defined in Table 6.7.3.3-2.

Table 6.7.3.3-1: UE Communication Statistics

Information	Description
UE group ID or UE ID	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7 or SUPI (see NOTE).
UE communications (1..max) (NOTE 1)	List of communication time slots.
> Periodic communication indicator (NOTE 1)	Identifies whether the UE communicates periodically or not.
> Periodic time (NOTE 1)	Interval Time of periodic communication (average and variance) if periodic. Example: every hour
> Start time (NOTE 1)	Start time observed (average and variance)
> Duration (NOTE 1)	Duration of communication (average and variance).
> Traffic characterization	S-NSSAI, DNN, ports, other useful information.
> Traffic volume (NOTE 1)	Volume UL/DL (average and variance).
> Ratio	Percentage of UEs in the group (in the case of a UE group).
Applications (0..max) (NOTE 1)	List of application in use.
> Application Id	Identification of the application.
> Start time	Start time of the application.
> Duration time	Duration interval time of the application.
> Occurrence ratio	Proportion for the application used by the UE during requested period.
> Spatial validity	Area where the service behaviour applies. If Area of Interest information was provided in the request or subscription, spatial validity may be a subset of the requested Area of Interest.
N4 Session ID (1..max)(NOTE 1)	Identification of N4 Session.
> Inactivity detection time	Value of session inactivity timer (average and variance).
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested" and "Preferred level of accuracy per analytics subset".	

Table 6.7.3.3-2: UE Communication Predictions

Information	Description
UE group ID or UE ID	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7 or SUPI (see NOTE).
UE communications (1..max) (NOTE 1)	List of communication time slots.
> Periodic communication indicator (NOTE 1)	Identifies whether the UE communicates periodically or not.
> Periodic time (NOTE 1)	Interval Time of periodic communication (average and variance) if periodic. Example: every hour.
> Start time (NOTE 1)	Start time predicted (average and variance).
> Duration time (NOTE 1)	Duration interval time of communication.
> Traffic characterization	S-NSSAI, DNN, ports, other useful information.
> Traffic volume (NOTE 1)	Volume UL/DL (average and variance).
> Confidence	Confidence of the prediction.
> Ratio	Percentage of UEs in the group (in the case of a UE group).
Applications (0..max)(NOTE 1)	List of application in use.
> Application Id	Identification of the application.
> Start time	Start time of the application.
> Duration time	Duration interval time of the application.
> Occurrence probability	Probability the application will be used by the UE.
> Spatial validity	Area where the service behaviour applies. If Area of Interest information was provided in the request or subscription, spatial validity may be a subset of the requested Area of Interest.
N4 Session ID (1..max)(NOTE 1)	Identification of N4 Session.
> Inactivity detection time	Value of session inactivity timer (average and variance).
> Confidence	Confidence of the prediction.
NOTE 1: Analytics subset that can be used in "list of analytics subsets that are requested" and "Preferred level of accuracy per analytics subset".	

NOTE: When Target of Analytics Reporting is an individual UE, one UE ID (i.e. SUPI) will be included, the NWDAF will provide the analytics communication result (i.e. list of (predicted) communication time slots) to NF service consumer(s) for the UE.

The results for UE groups address the group globally. The ratio is the proportion of UEs in the group for a given communication at a given time and duration.

The number of UE communication entries (1..max) is limited by the maximum number of objects provided as part of Analytics Reporting Information. The communications shall be provided by order of time, possibly overlapping.

Depending on the list size limitation, the least probable communications on a given Analytics target period may not be provided.

6.7.3.4 Procedures

The NWDAF can provide UE communication related analytics, in the form of statistics or predictions or both, to a 5GC NF.

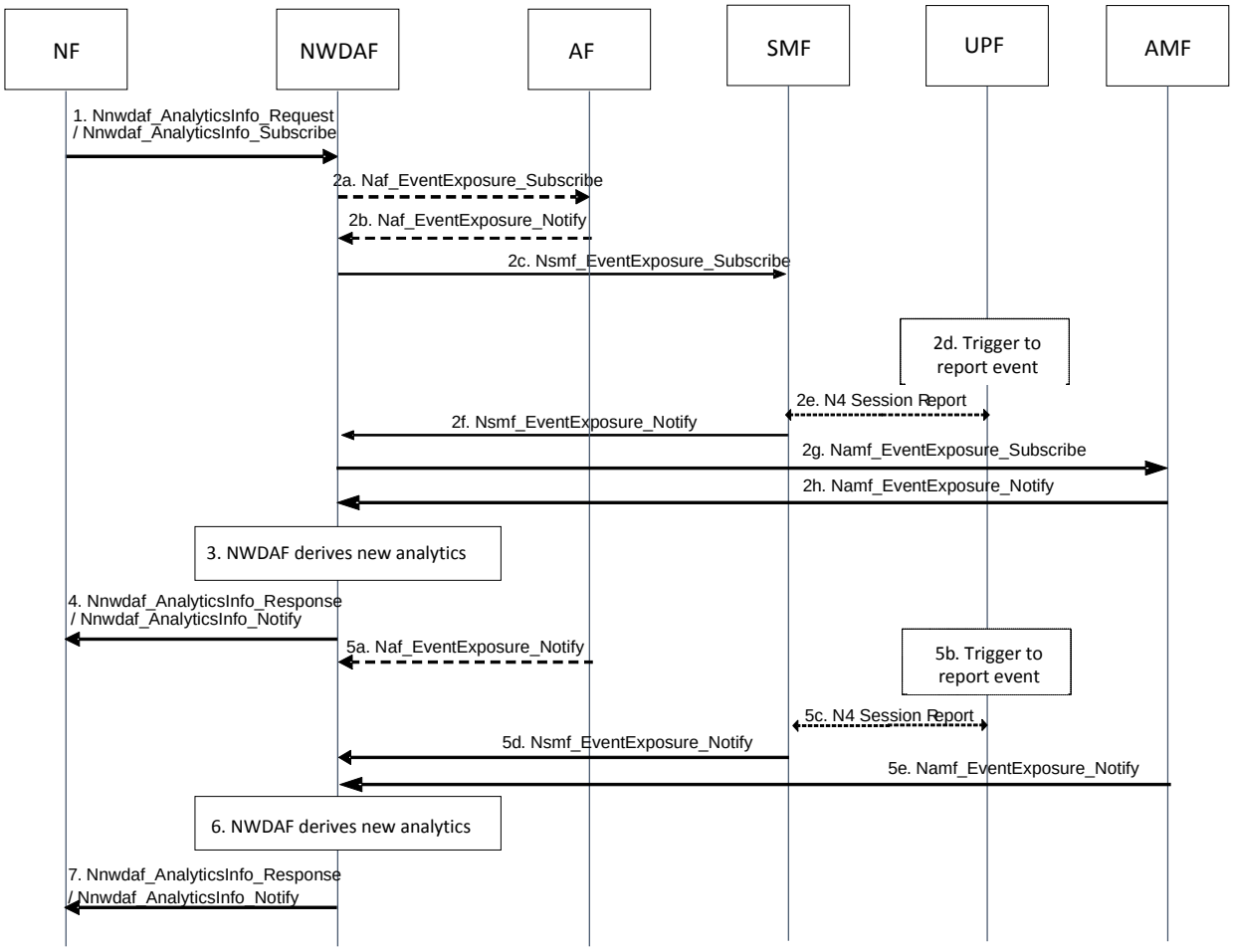

Figure 6.7.3.4-1: Procedure for UE communication analytics

1. 5GC NF to NWDAF: Nnwdaf_AnalyticsSubscription_Subscribe (Analytics ID=UE communication, Target of Analytics Reporting=SUPI, Analytics Filter Information = (Application ID, Area of Interest, etc.)).

   5GC NF sends a request to the NWDAF for analytics on a specific UE(s), using either Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription_Subscribe service. The analytics type indicated by "Analytics ID" is set to "UE communication". The Target of Analytics Reporting is set to SUPI or an Internal Group Identifier and Analytics Filter may include Application ID and Area of Interest.

2a-b. NWDAF to AF (Optional): Naf_EventExposure_Subscribe (Event ID, external UE ID, Application ID, Area of Interest).

   In order to provide the requested analytics, the NWDAF may subscribe per application communication information, which is identified by Application ID, from AFs for the UE. The Event ID "UE Communication information" as defined in TS 23.502 [3] is used, which indicates communication report for the UE which is requested by the 5GC NF in the step 1. The external UE ID is obtained by the NWDAF based on UE internal ID, i.e. SUPI. In the case of external AF, the NEF translates the requested Area of Interest into a list of geographic zone identifier(s) as described in clause 5.6.7.1 of TS 23.501 [2].

   This step is skipped if the NWDAF already has the requested analytics available or has subscribed to the AF.

2c. NWDAF to SMF: Nsmf_EventExposure_Subscribe (Event ID, SUPI, Application ID).

   In order to provide the requested analytics, the NWDAF subscribes to information of the UE and may subscribe to N4 Session related input data from SMFs as defined in Table 6.7.3.2-1.

2d-e. N4 related input data is provided by UPF to SMF.

NOTE: The NWDAF request does not trigger any N4 session Establishment/Modification procedure. N4 session related input is only retrieved if UPF has already been triggered to send reports. UPF sends N4 session level reports, including PDU session Inactivity to SMF, according to clause 4.4.2.2 of TS 23.502 [3].

2f. SMF provides the requested input data to NWDAF.

2g-h. NWDAF to AMF: Namf_EventExposure_Subscribe (Event ID, SUPI, Area of Interest).

In order to provide the requested analytics, the NWDAF retrieves one or more of Type Allocation code, UE connection management state, UE access behaviour trends and UE location trends from AMF.

NOTE: The NWDAF determines the SMF serving the UE as described in clause 6.2.2.1.

3. The NWDAF derives requested analytics, in the form of UE communication statistics or predictions or both.

4. NWDAF to 5GC NF: Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify.

The NWDAF provides requested UE communication analytics to the NF, using either Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1.

5-7. If the NF subscribed UE communication analytics at step 1, when the NWDAF generates new analytics, it notifies the new generated analytics to the 5GC NF.

6.7.4 Expected UE behavioural parameters related network data analytics

6.7.4.1 General

The clause 6.7.4 defines how a service consumer learns from the NWDAF the expected UE behaviour parameters as defined in clause 4.15.6.3 ofTS 23.502 [3] for a group of UEs or a specific UE.

The service consumer may be an NF (e.g. AMF, UDM, AF), or the OAM.

The consumer of these analytics shall indicate in the request:

- Analytics ID = "UE Mobility" or "UE Communication".
- Target of Analytics Reporting: a single UE (SUPI) or a group of UEs (an Internal Group ID).

NOTE: In the case of untrusted AF the Target of Analytics Reporting can be a GPSI or an External Group Identifier that is mapped in the 5GC to a SUPI or an Internal Group Identifier

- An Analytics target period, which indicates the time period over which the statistics or predictions are requested.
- Analytics Filter Information optionally including:
  - Area of Interest (AOI);
  - S-NSSAI;
  - DNN;
  - Application ID;
  - an optional list of analytics subsets that are requested (see clause 6.7.3.3).
- Optional maximum number of objects.
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

The NWDAF shall notify the result of the analytics to the consumer as indicated in clause 6.7.4.3.

6.7.4.2 Input Data

In order to produce "UE Mobility" analytics, the NWDAF collects UE mobility information, UE location trends and/or UE access behaviour trends, as defined in clause 6.7.2.2.
In order to produce "UE Communication" analytics, the NWDAF collects UE communication information, UE communication trends, UE session behaviour trends and/or UE access behaviour trends, as defined in clause 6.7.3.2.

6.7.4.3 Output Analytics

The analytics results for "UE Mobility" are specified in Table 6.7.2.3-1 and Table 6.7.2.3-2.

The analytics results for "UE Communication" are specified in Table 6.7.3.3-1 and Table 6.7.3.3-2.

6.7.4.4 Procedures

6.7.4.4.1 NWDAF-assisted expected UE behavioural analytics

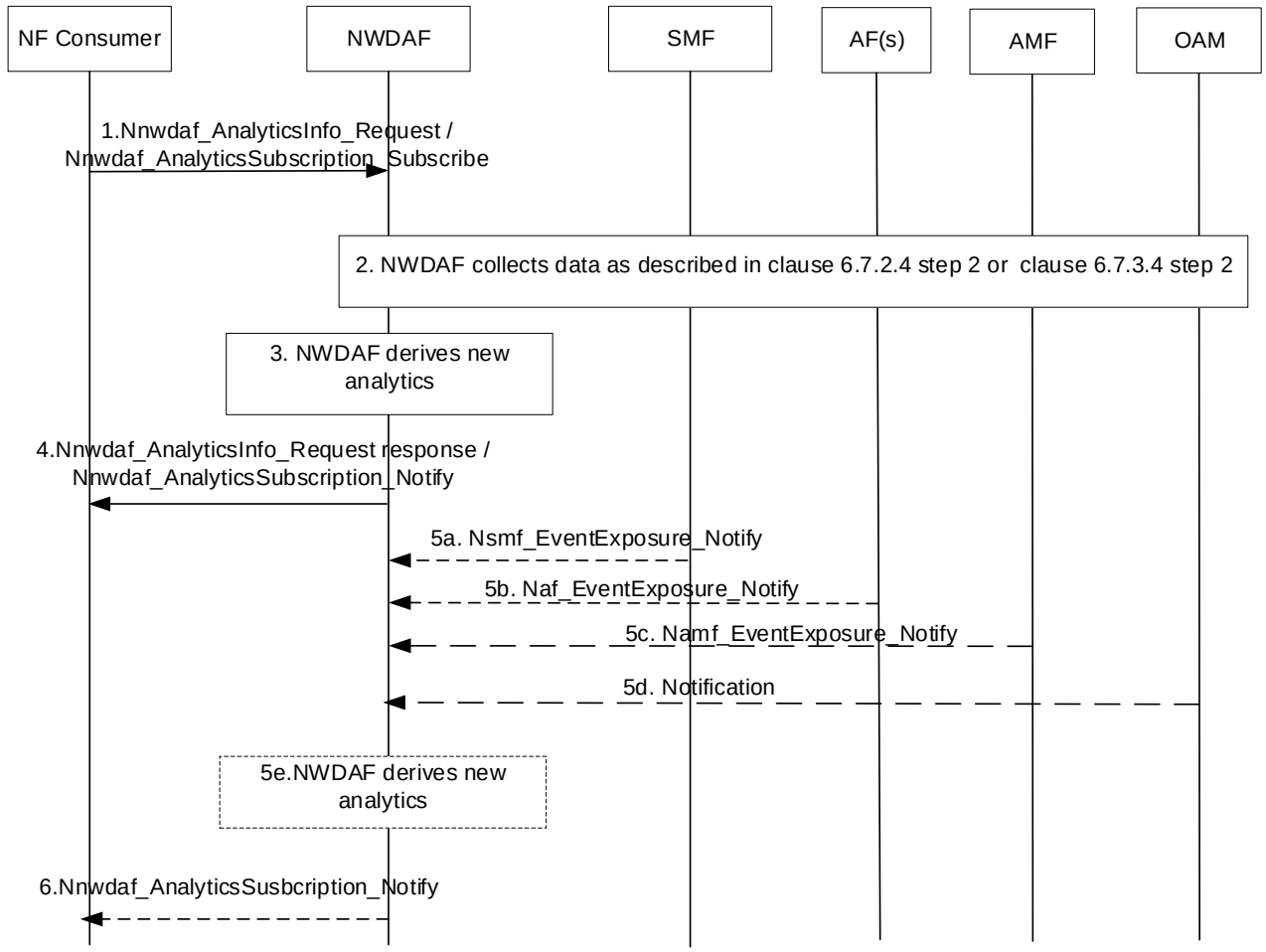

Figure 6.7.4.4.1-1: NWDAF assisted expected UE behavioural analytics procedure

1. 5GC NF (e.g. AMF, SMF, AF and UDM) to NWDAF: Nnwdaf_AnalyticsInfo_Request (Analytics ID, Target of Analytics Reporting, Analytics Filter Information) or Nnwdaf_AnalyticsSubscription_Subscribe (Analytics ID, Target of Analytics Reporting, Analytics Filter Information).

   The Analytics ID is set to "UE Mobility" or to "UE Communication"," and the consumer request analytics.

2. If Analytics ID is set to "UE Mobility", the NWDAF collects data from OAM, AMF and/or AF as specified in clause 6.7.2.4 step 2, unless the information is already available.

If Analytics ID is set to "UE Communication", the NWDAF collects data from AMF, SMF and/or AF as specified in clause 6.7.3.4 step 2, unless the information is already available.

3. The NWDAF derives requested analytics.

4. NWDAF to 5GC NF: Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify.

   The NWDAF provides requested Expected UE behaviour to the NF, using either Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1.

5-6. If the NF subscribed to at step 1, when the NWDAF generates new analytics, it provides the new generated analytics to the NF.

6.7.5 Abnormal behaviour related network data analytics

6.7.5.1 General

This clause defines how to identify a group of UEs or a specific UE with abnormal behaviour, e.g. being misused or hijacked, with the help of NWDAF.

NOTE 1: The misused or hijacked UEs are UEs in which there are malicious applications running or UEs which have been stolen.

The consumer of this analytics could be a 5GC NF. The 5GC NF subscribes analytics on abnormal behaviour from a NWDAF based on the UE subscription, network configuration or application layer request.

The NWDAF performs data analytics on abnormal behaviour if there is a related subscription and returns exception reports that result from the analysis of the correlations between behavioural variables. The exception reports contain an Exception Level expressed in the form of a scalar value, possibly supplemented by additional measurements.

The consumer of this analytics shall indicate in the request:

- Analytics ID = "Abnormal behaviour";
- Target of Analytics Reporting: a single UE, any UE or an Internal Group Identifier;
- An Analytics target period indicates the time period over which the statistics or predictions are requested;
- Analytics Filter Information optionally including:
  - expected UE behaviour parameters;
  - expected analytics type or list of Exception IDs with associated thresholds for the Exception Level, where the expected analytics type can be mobility related, communication related or both;
  - Area of interest;
  - Application ID;
  - DNN;
  - S-NSSAI.

NOTE 2: The expected analytics type generally indicates whether mobility or communication related abnormal behaviour analytics or both are expected by the consumer, and the list of exception IDs indicates what specific analytics are expected by the consumer. Either the expected analytics type or the list of Exception IDs needs to be indicated, but they are not presented simultaneously. When the expected analytics type is indicated, the NWDAF performs corresponding abnormal behaviour analytics which are supported by the NWDAF. The relation between the expected analytics type and Exception IDs is defined in Table 6.7.5.1-1.

- Optionally, maximum number of objects and maximum number of SUPIs;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

Table 6.7.5.1-1: Relation between expected analytics type and Exception IDs

Expected analytics type	Exception IDs matching the expected analytics type
mobility related	Unexpected UE location, Ping-ponging across neighbouring cells, Unexpected wakeup, Unexpected radio link failures.
communication related	Unexpected long-live/large rate flows, Unexpected wakeup, Suspicion of DDoS attack, Wrong destination address, Too frequent Service Access.

If the Target of Analytics Reporting is any UE, then the Analytics Filter should at least include:

- Area of Interest or S-NSSAI, if the expected analytics type or the list of Exception IDs is mobility related.
- Area of Interest, application ID, DNN or S-NSSAI, if the expected analytics type or the list of Exception IDs is communication related.

If the Target of Analytics Reporting is any UE, the consumer of this analytics shall request either mobility related only or communication related only abnormal behaviour analytics, but not both at the same time.

The expected UE behaviour parameters that the consumer can indicate in the request when known depend on the Exception ID that the consumer expects. They may encompass UE behaviour parameters as defined inclause 4.15.6.3 ofTS 23.502 [3] and other parameters. Table 6.7.5.1-2 shows the mapping between each Exception ID and UE behaviour parameters.

Table 6.7.5.1-2: Description of Expected UE Behaviour parameters per Exception ID

Exception ID	UE behaviour parameters to provide
Unexpected UE location	Expected UE Moving Trajectory Stationary Indication
Unexpected long-live/large rate flows	Periodic Time Scheduled Communication Time Communication Duration Time
Unexpected wakeup	Periodic Time Communication Duration Time Scheduled Communication Time
Suspicion of DDoS attack	Periodic Time Communication Duration Time Scheduled Communication Time Scheduled Communication Type Traffic Profile Expected transaction Dispersion
Too frequent Service Access	Periodic Time
Unexpected radio link failures	Expected UE Moving Trajectory
Ping-ponging across neighbouring cells	Expected UE Moving Trajectory Stationary Indication

When the NWDAF detects those UEs that deviate from the expected UE behaviour, e.g. unexpected UE location, abnormal traffic pattern, unexpected transaction dispersion amount, wrong destination address, etc. the NWDAF shall notify the result of the analytics to the consumer as specified in clause 6.7.5.3.

6.7.5.2 Input Data

The Exceptions information from AF is as specified in Table 6.7.5.2-1.

On request of the service consumer, the NWDAF shall collect and analyse UE behavioural information from the 5GC NFs (SMF, AMF, AF), or OAM as specified in clauses 6.7.2.2 and 6.7.3.2 and/or expected UE behavioural parametersfrom UDM as defined in clause 4.15.6.3, TS 23.502 [3], depending on Exception IDs.

NOTE: Care needs to be taken with regards to load by avoiding to cause major extra signalling when collecting data for any UE.

Table 6.7.5.2-1: Exceptions information from AF

Information	Description
IP address 5-tuple	To identify a data flow of a UE via the AF (such as the Firewall or a Threat Intelligence Sharing platform)
Exceptions (1..max) (NOTE 1)	
>Exception ID	Indicating the Exception ID (such as Unexpected long-live/large rate flows and Suspicion of DDoS attack as defined in Table 6.7.5.3-2) of the data flow.
>Exception Level	Scalar value indicating the severity of the abnormal behaviour.
>Exception trend	Measured trend (up/down/unknown/stable)
NOTE 1: The Exceptions information and the UE behavioural information as defined in clauses 6.7.2.2 and 6.7.3.2could help NWDAF to train an Abnormal classifier, which could be used to classify a UE behaviour data into Normal behaviour or Exception.	

6.7.5.3 Output Analytics

Corresponding to the "abnormal behaviour" Analytics ID, the analytics result provided by the NWDAF is defined in Table 6.7.5.3-1 and Table 6.7.5.3-2.Whenthe level of an exception trespasses above or below the threshold, the NWDAF shall notify the consumer with the exception ID associated with the exception if the exception ID is within the list of exception IDs indicated by the consumer or matches the expected analytics type indicated by the consumer. The NWDAF shall provide the Exception Level and determine which of the other information elements to provide, depending on the observed exception.

Abnormal behaviour statistics information is defined in Table 6.7.5.3-1.

Table 6.7.5.3-1: Abnormal behaviour statistics

Information	Description
Exceptions (1..max)	List of observed exceptions
>Exception ID	The risk detected by NWDAF
> Exception Level	Scalar value indicating the severity of the abnormal behaviour
> Exception trend	Measured trend (up/down/unknown/stable)
> UE characteristics	Internal Group Identifier, TAC
> SUPI list (1..SUPImax)	SUPI(s) of the UE(s) affected with the Exception
> Ratio	Estimated percentage of UEs affected by the Exception within the Target of Analytics Reporting
> Amount	Estimated number of UEs affected by the Exception (applicable when the Target of Analytics Reporting = "any UE")
> Additional measurement	Specific information for each risk (see Table 6.7.5.3-3)

Abnormal behaviour predictions information is defined in Table 6.7.5.3-2.

Table 6.7.5.3-2: Abnormal behaviour predictions

Information	Description
Exceptions (1..max)	List of predicted exceptions
>Exception ID	The risk detected by NWDAF
> Exception Level	Scalar value indicating the severity of the abnormal behaviour
> Exception trend	Measured trend (up/down/unknown/stable)
> UE characteristics	Internal Group Identifier, TAC
> SUPI list (1..SUPImax)	SUPI(s) of the UE(s) affected with the Exception
> Ratio	Estimated percentage of UEs affected by the Exception within the Target of Analytics Reporting
> Amount	Estimated number of UEs affected by the Exception (applicable when the Target of Analytics Reporting = "any UE")
> Additional measurement	Specific information for each risk (see Table 6.7.5.3-3)
> Confidence	Confidence of this prediction

The UE characteristics may provide a set of features common to all UEs affected with the exception.

The number of exceptions and the length of the SUPI list shall respectively be lower than the parameters maximum number of objects and Maximum number of SUPIs provided as part of Analytics Reporting Information.

If PCF subscribes to notifications on "Abnormal behaviour", the NWDAF shall send the PCF notifications about the risk, which may trigger the PCF to update the AM/SM policies.

The NWDAF also sends the notification directly to the AMF or SMF, if the AMF or SMF subscribes to the notification, so that the AMF or SMF may, based on operator local policies defined on a per S-NSSAI basis (for AMF) or on a per S-NSSAI, per DNN, or per (DNN,S-NSSAI) basis (for SMF), take actions for risk solving.

If the AF subscribes to notifications on "Abnormal behaviour", the NWDAF sends the notifications to the AF so that the AF may take actions for risk solving.

The following Table 6.7.5.3-3 gives examples of additional measurement provided by the NWDAF and examples of NF actions for solving each risk.

Table6.7.5.3-3:Examples of additional measurements and NF actions for risk solving

Exception ID and description	Additional measurement	Actions of NFs
Unexpected UE location	Unexpected UE location (TA or cells which the UE stays)	PCF may extend the Service Area Restrictions with current UE location. AMF may extend the mobility restriction with current UE location.
Ping-ponging across neighbouring cells	Numbers, frequency, time and location information, assumption about the possible circumstances of the ping-ponging	If the ping-ponging are per UE, then: 1. the AMF may adjust the UE (e.g. a stationary UE) registration area. 2. the AMF and/or the AF may allow the use of Coverage Enhancement for the affected UE.
Unexpected long-live/large rate flows	Unexpected flow template (IP address 5 tuple)	SMF updates the QoS rule, e.g. decrease the MBR for the related QoS flow. PCF, if dynamic PCC applies for corresponding DNN, S-NSSAI, updates PCC Rules that triggers SMF updates the QoS rule, e.g. decrease the MBR for the related QoS flow.
Unexpected wakeup	Time of unexpected wake-up	AMF applies MM back-off timer to the UE.
Suspicion of DDoS attack	Victim's address (target IP address list)	PCF may request SMF to release the PDU session. SMF may release the PDU session and apply SM back-off timer.
Wrong destination address	Wrong destination address (target IP address list)	PCF updates the packet filter in the PCC Rules that triggers the SMF to update the related QoS flow and configures the UPF.
Too frequent Service Access	Volume, frequency, time, assumptions about the possible circumstances	AF may release the AF session. PCF may request SMF to release the PDU session. SMF may release the PDU session and apply SM back-off timer.
Unexpected radio link failures	Numbers, frequency, time and location, assumptions about the possible circumstances	If the unexpected radio link failures are per UE location bases, the AMF may allow the use of CE (Coverage Enhancement) in the affected location. Also, the Operator may improve the coverage conditions in the affected location. If the unexpected radio link failures are per UE bases, then the AMF and/or the AF may allow the use of CE for the affected UE.

6.7.5.4 Procedure

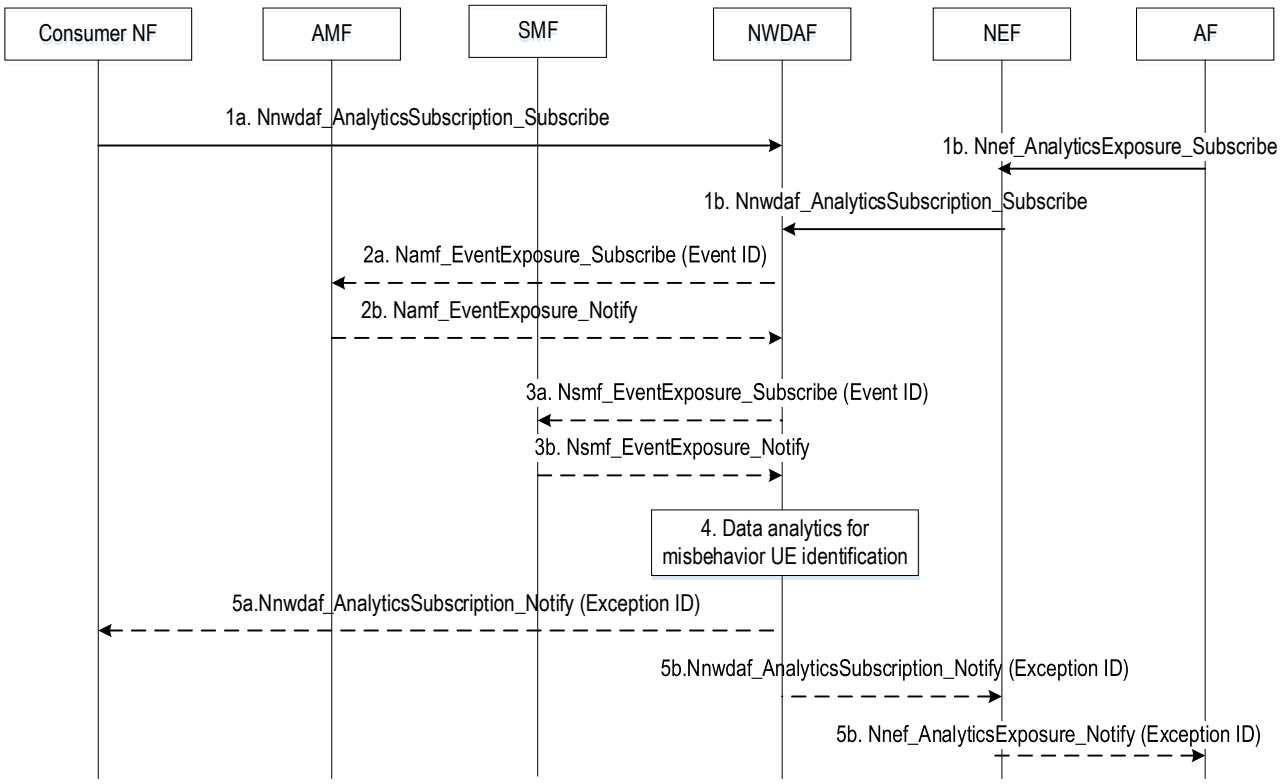

Figure 6.7.5.4-1: Procedure for NWDAF assisted misused or hijacked UEsidentification

1a. A consumer NF subscribes to/requests NWDAF using Nnwdaf_AnalyticsSubscription_Subscribe/ Nnwdaf_AnalyticsInfo_Request (Analytics ID = Abnormal behaviour, Target of Analytics Reporting =Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information).

A consumer NF may subscribe to/request abnormal behaviour notification/response from NWDAF for a group of UEs, any UE or a specific UE. The Analytics ID indicates the NWDAF to identify misused or hijacked UEs through abnormal behaviour analytic.

1b. AF to NWDAF: Nnwdaf_AnalyticsSubscription_Subscribe or Nnwdaf_AnalyticsInfo_Request (Analytics ID, Target of Analytics Reporting = External-group identifier, any UE or External UE ID, Analytics Filter Information).

For untrusted AFs, the AF sends the subscription via a NEF, where the AF invokes NEF service Nnef_AnalyticsExposure_Subscribe or Nnef_AnalyticsExposure_Fetch (Analytics ID, Target of Analytics Reporting = External-group-identifier, any UE or External UE ID, Analytics Filter Information).

An AF may also subscribe to/request abnormal behaviour notification/response from NWDAF for a group of UEs, a specific UE or any UE, where the subscription/request message may contain expected UE behaviour parameters identified on the application layer. If an External-Group-Identifier is provided by the AF, the NEF interrogates UDM to map the External-Group-Identifier to the Internal-Group-Identifier and obtain SUPI list corresponding to the Internal-Group-Identifier.

2. [Conditional] NWDAF to AMF:Namf_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI).

The NWDAF sends subscription requests to the related AMF to collect UE behavioural information if it has not subscribed such data.

NOTE 1: The NWDAF determines the related AMF(s) as described in clause 6.2.2.1.

The AMF sends event reports to the NWDAF based on the report requirements contained in the subscription request received from the NWDAF.

If requested by NWDAF via Event Filter(s), the AMF checks whether the UE's behaviour matches its expected UE behavioural information. In this case, the AMF sends event reports to the NWDAF only when it detects that the UE's behaviour deviated from its expected UE behaviour.

Depending on the Exception ID, the NWDAF may in addition perform data collection from OAM as specified in clause 6.2.3.2.

3. [Conditional] NWDAF to SMF:Nsmf_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI).

   The NWDAF sends subscription requests to the related SMF(s) if it has not subscribed to such data.

NOTE 2: Besides Analytics Filter Information, other mechanisms such as setting maximum number of SUPIs, and/ or using sampling ratio as part of Analytics Reporting Parameters as per Event Reporting Information (clause 4.15.1 ofTS 23.502 [3]) can be used by the analytics consumer to limit signalling load, e.g. when the Target of Analytics Reporting is "any UE". The NWDAF can also use sampling ratio, possibly with partition criteria, when subscribing towards AMF and SMF.

NOTE 3: The NWDAF determines the related SMF(s) as described in clause 6.2.2.1.

The SMF sends event reports to the NWDAF based on the report requirements contained in the subscription request received from the NWDAF.

If requested by NWDAF via Event Filter(s), the SMF checks whether the UE's behaviour matches its expected UE behavioural information. In this case, the SMF sends event reports to the NWDAF only when it detects that the UE's behaviour deviated from its expected UE behaviour.

4. The NWDAF performs data analytics for misused or hijacked UEs identification. Based on the analytics and operator's policies the NWDAF determines whether to send a notification to the consumer NF or AF.

5a. [Conditional] NWDAF to consumer NF (AMF or PCF or SMF depending on the subscription): Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Response (Analytics ID, Exception ID, Internal-Group-Identifier or SUPI, Exception level) (which is used depending on the service used in step 1a).

   If the NWDAF determines to send a notification/response to the consumer 5GC NFs, the NWDAF invokes Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response service operations. Based on the notification/response, the 5G NFs adopt configured actions to resolve/mitigate/avoid the risks as described in the Table 6.7.5.3-1.

5b. [Conditional] NWDAF to AF: Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response (Analytics ID, Exception ID, External UE ID, Exception level) (which is used depending on the service used in step 1b).

   If the NWDAF determines to send a notification/response to the consumer AF, the NWDAF needs to include external UE ID of the identified UE into the notification/response message.

NOTE 3: Based on the notification, the AF can adopt corresponding actions, e.g. adjusting recommended TCP Window Size, adjusting recommended Service Start and End.

NOTE 4: The call flow only shows a subscribe-notify model for the interaction of NWDAF and consumer NF for simplicity instead of both request-response model and subscription-notification model.

6.8 User Data Congestion Analytics

6.8.1 General

The NWDAF can provide user data congestion related analytics, by one-time reporting or continuous reporting, in the form of statistics or predictions or both, to another NF. User Data Congestion related analytics can relate to congestion experienced while transferring user data over the control plane or user plane or both. A request for user data congestion analytics relates to a specific area or to a specific user. If the consumer of these analytics provides a UE ID, the NWDAF determines the area where the UE is located. The NWDAF then collects measurements per cell and uses the measurements to determine user data congestion analytics.

The request for user data congestion related analytics indicates the location area information where congestion related analytics is desired or indicates a UE Identity that can be used by the NWDAF to determine the location area information where congestion related analytics is desired. When requesting user data congestion, the consumer may request the identifiers of the applications that contribute the most to the traffic in the area. The consumer may indicate how many applications should be reported by providing the maximum number of applications in the request or subscription.

When the consumer of user data congestion related analytics subscribes to user data congestion related analytics, it may indicate a threshold and the NWDAF will provide analytics to the consumer when the congestion level crosses the threshold. The consumer can indicate an S-NSSAI in the request when congestion analytics are needed on a per slice level.

The service consumer may be an NF (e.g. NEF, AF, PCF).

The consumer of these analytics may indicate in the request or subscription the following parameters, its content is described in the clause 6.1.3:

- Analytics ID = "User Data Congestion".
- Target of Analytics Reporting: either a single UE (SUPI), or "any UE".

NOTE: The Target of Analytics Reporting set to "any UE" applies when user data congestion analytics relates to a specific Area of Interest.

- Analytics Filter Information:
  - Area of Interest (i.e. list of TAIs or CellIDs) which restricts the area in focus (mandatory if Target of Analytics Reporting is set to "any UE", optional otherwise);
  - an optional list of analytics subsets that are requested, (see clause 6.8.3);
  - Optional S-NSSAI, in order to obtain congestion analytics only on a given slice.
- Optional Reporting Threshold, which applies only for subscriptions and indicates conditions on the congestion level (Network Status Indication, see clause 6.8.3) to be reached in order to be notified by the NWDAF.
- Preferred level of accuracy of the analytics;
- Preferred order of results for the list of User Data Congestion statistics or predictions:
  - ordering by Applicable Time Window, chronological or reverse chronological order; or
  - ordering by Network Status Indication, ascending or descending;
- Optional maximum number of objects;
- An Analytics target period indicates the time period over which the statistics or prediction are requested, either in the past or in the future.
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

The NWDAF notifies the result of the analytics to the consumer as indicated in clause 6.8.3.

6.8.2 Input data

The detailed information collected by the NWDAF is defined in Table 6.8.2-1.

NOTE 1: Performance Measurements defined in TS 28.552 [8] represent resource utilisation but do not, by themselves, indicate the event of congestion or congestion levels. The NWDAF collects measurements from the OAM and how the NWDAF derives Network Status Indication (NSI) is not specified.

Table 6.8.2-1: Data Collected from the NF and OAM related to User Data Congestion Analytics

Information	Source	Description
UE Location	AMF	UE location information that NWDAF can use to derive the Area of Interest.
Measurements	OAM	Performance Measurements that will be used by the NWDAF to determine congestion levels. Performance Measurements are related to information transfer over the user plane and/or the control plane (e.g. UE Throughput, DRB Setup Management, RRC Connection Number, PDU Session Management, and Radio Resource Utilization as defined in TS 28.552 [8]). The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

Table 6.8.2-2: Data Collected from the UPF or from the AF related to User Data Congestion Analytics

Information	Source	Description
Application ID	UPF or AF	Application identifier as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 1).
IP Packet Filter Set	UPF or AF	IP Packet Filter set as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 1).
Measurement period	UPF or AF	Measurement period.
Throughput UL/DL	UPF or AF	Average Throughput UL/DL over the measurement period.
Throughput UL/DL (peak)	UPF or AF	Peak Throughput UL/DL over the measurement period.
Timestamp	UPF or AF	Time when measurements are taken.
Achieved sampling ratio	UPF	Sampling ratio achieved by UPF (see NOTE 2).
NOTE 1: Application Id and IP Packet Filter Set are mutually exclusive. NOTE 2: UPF may apply data sampling to reduce the load on the UPF. This parameter is provided when no sampling ratio is configured at the UPF or the UPF could not fulfil the configured sampling ratio. NOTE 3: Multiple outputs are provided by the UPF when multiple Service Data Flows are running at the UPF for the same UE and measurement period. NOTE 4: How NWDAF collects information from UPF is not defined in this Release of the specification.		

NOTE 2: Care needs to be taken with regards to load and major signalling caused when requesting "any UE". This can be achieved via utilization of event filters (e.g. Area of Interest), Analytics Reporting Information (e.g. maximum number of objects), or preferred sampling ratio provided by NWDAF to the UPF and/or local UPF configuration of data collection for specific application IDs, Packet Filter Sets and/or PFDs.

Additionally, NWDAF may use statistics or predictions on service experience as specified in clause 6.4.3 as an input, e.g. for service experience in a given area or service experience for some specific applications such as high bandwidth applications.

6.8.3 Output analytics

The NWDAF outputs the user data congestion analytics for transfer over the user plane, for transfer over the control plane, or for both. The output may consist of statistics, predictions, or both. The detailed information provided by the NWDAF is defined in Table 6.8.3-1 for statistics and in Table 6.8.3-2 for predictions.

Table 6.8.3-1: User Data Congestion statistics

Information	Description
Area of Interest	A list of TAIs or Cell IDs
List of user data congestion Analytics (1..max)	List of user data congestion Analytics. See NOTE 5.
>Type	User Plane or Control Plane
>Applicable Time Window	The time period that the analytics applies to
>Network Status Indication	Congestion Level
> List of top applications in UL (0..N_U) (NOTE 1, NOTE 4)	The list of applications that contribute the most to the traffic in the UL direction.
>> Application ID	Application identifier as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 2).
>> IP Packet Filter Set	IP Packet Filter set as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 2).
>> Percentage	The application's throughput as a percentage of the total throughput in the Area of Interest.
> List of top applications in DL (0..N_D) (NOTE 1, NOTE 4)	The list of applications that contribute the most to the traffic in the DL direction.
>> Application ID	Application identifier as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 2)
>> IP Packet Filter Set	IP Packet Filter set as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 2).
>> Percentage	The application's throughput as a percentage of the total throughput in the Area of Interest.

NOTE 1: This information element is an Analytics subset that can be used in "list of analytics subsets that are requested".
NOTE 2: Application Id and IP Packet Filter Set are mutually exclusive.
NOTE 3: The listed applications are not necessarily ranked by any order of traffic contribution.
NOTE 4: This information element relates to congestion experienced while transferring user data over the user plane.
NOTE 5: The number of user data congestion analytics entries is limited by the maximum number of objects provided as part of Analytics Reporting Information.

Table 6.8.3-2: User Data Congestion predictions

Information	Description
Area of Interest	A list of TAIs or Cell IDs.
List of user data congestion Analytics (1..max)	List of user data congestion Analytics. See NOTE 5.
>Type	User Plane or Control Plane.
>Applicable Time Window	The time period that the analytics applies to.
>Network Status Indication	Congestion Level.
> Confidence	Confidence of this prediction.
> List of top applications in UL (0..N_U) (NOTE 1, NOTE 4)	The list of applications predicted to contribute most of the traffic in the UL direction.
>> Application ID	Application identifier as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 2).
>> IP Packet Filter Set	IP Packet Filter set as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 2).
>> Percentage	The application's throughput as a percentage of the total throughput in the Area of Interest.
>> Confidence	Confidence of this prediction.
> List of top applications in DL (0..N_D) (NOTE 1, NOTE 4)	The list of applications predicted to contribute most of the traffic in the DL direction.
>> Application ID	Application identifier as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 2).
>> IP Packet Filter Set	IP Packet Filter set as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 2).
>> Percentage	The application's throughput as a percentage of the total throughput in the Area of Interest.
>> Confidence	Confidence of this prediction.
NOTE 1: This information element is an Analytics subset that can be used in "list of analytics subsets that are requested". NOTE 2: Application Id and IP Packet Filter Set are mutually exclusive. NOTE 3: The listed applications are not necessarily ranked by any order. NOTE 4: This information element relates to congestion experienced while transferring user data over the user plane. NOTE 5: The number of user data congestion analytics entries is limited by the maximum number of objects provided as part of Analytics Reporting Information.	

The following list shows the applicability of the analytics subsets per consumer:

- Analytics subset "List of top applications in UL (0..NU)" and "List of top applications in DL (0..ND)" are applicable to any consumer (e.g. PCF, AF, NEF), The NWDAF decides if these Analytics subset is provided to an AF.

6.8.4 Procedures

6.8.4.1 Procedure for one-time or continuous reporting of analytics for user data congestion in a geographic area

The procedure as depicted in Figure 6.8.4.1-1 is used by an NF to retrieve congestion analytics for a specific geographic area. The procedure can be used to request a one-time or continuous reporting of congestion analytics.

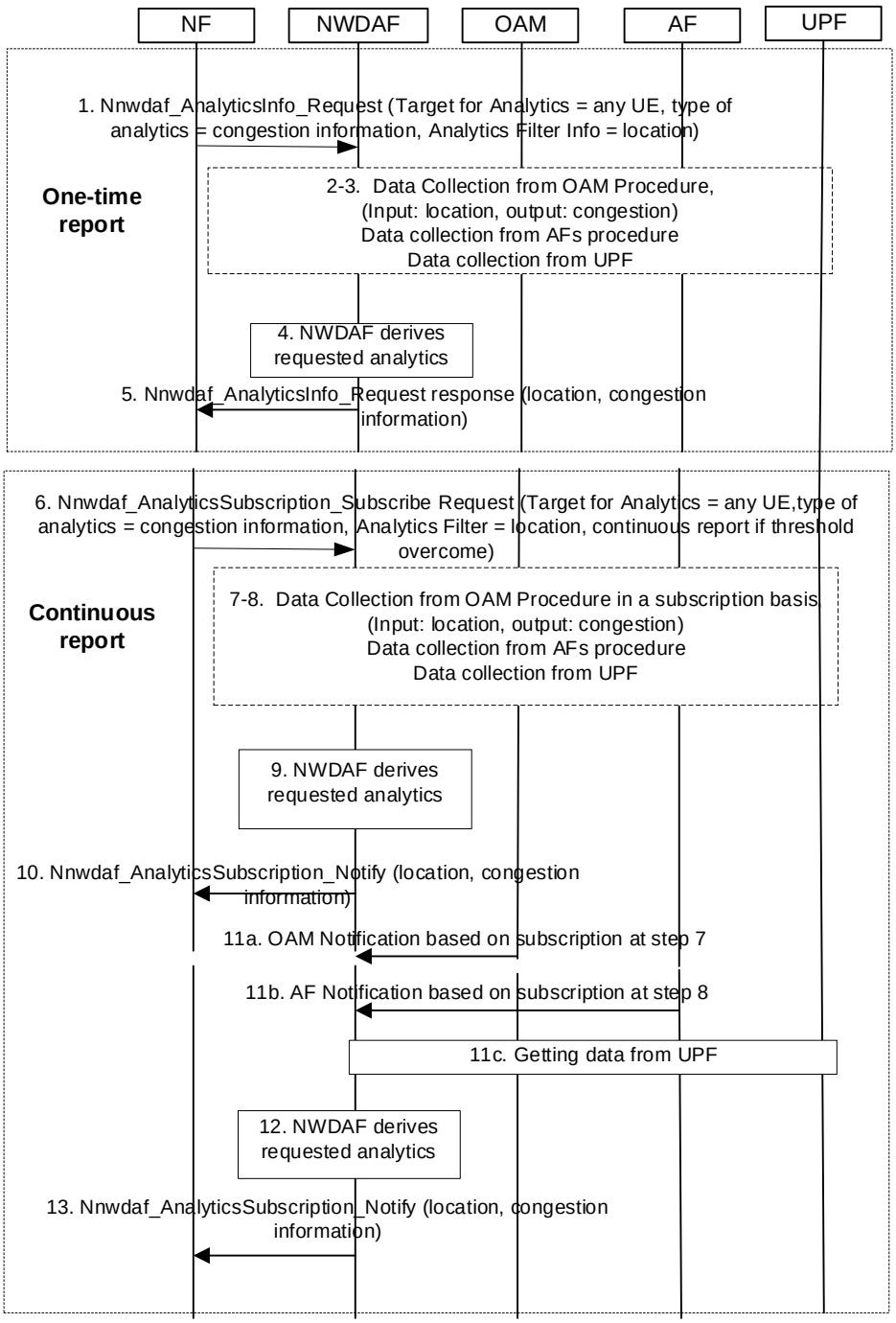

Figure 6.8.4.1-1: Procedure for one-time or continuous reporting of analytics for congestion in a geographic area

For one-time reporting:

1. The NF sends Nnwdaf_AnalyticsInfo_Request to NWDAF, indicating request for analytics for congestion in a specific location. The NF can request statistics or predictions or both. The Analytics ID is set to "User Data Congestion" for transfer over user plane, control plane, or both, the Target of Analytics Reporting is set to "any UE" and Analytics Filter Information set to include a location (e.g. ECGI, TA) and an indication to provide the list of applications that contribute the most to the traffic.

2-3. If the request is authorized, and in order to provide the requested analytics, the NWDAF may request the measurement information for the requested location from OAM services following the data collection from

OAM procedure as captured in 6.2.3.2. If the NWDAF already has information about the requested location, these steps are omitted. The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

If the request is to provide the list of applications that contribute the most to the traffic, then the NWDAF collects input data from the AF for the applications being served by AF(s) by invoking Naf_EventExposure_Subscribe service or Nnef_EventExposure_Subscribe (if via NEF) or collected from the UPF or collected from both, AF and UPF.

4. The NWDAF derives requested analytics.

5. The NWDAF provides the analytics for congestion to the NF.

For continuous reporting:

6. The NF sends Nnwdaf_AnalyticsSubscription_Subscribe Request to the NWDAF, indicating request for analytics for congestion in a specific location (e.g. ECGI, TA), possibly with thresholds and including an indication to provide the list of applications that contribute the most to the traffic. The NF can request statistics or predictions or both. The type of analytics is set to user data congestion analytics for transfer over user plane, control plane, or both.

7-8. The NWDAF subscribes to OAM services following the data collection from OAM procedure as captured in 6.2.3.2 to get measurement information for the requested location, possibly providing measurement thresholds for example, data congestion crossing values. The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7]. If a request is to provide the list of applications that contribute the most to the traffic, the NWDAF subscribes to the service data from AF by invoking Naf_EventExposure_Subscribe service or Nnef_EventExposure_Subscribe (if via NEF) or from the UPF or from both.

9. The NWDAF derives requested analytics.

10. The NWDAF provides the analytics for congestion to the NF.

11a. A change of user data congestion status corresponding to crossing a threshold set by the NWDAF at steps 7-8 is detected by OAM and notified to NWDAF.

11b. The AF notifies the NWDAF with the input data as defined in table 6.8.2-2.

11c. The UPF provides the NWDAF with the input data as defined in table 6.8.2-2.

12. The NWDAF derives new analytics.

13. The NWDAF provides a notification for analytics for the user data congestion to the NF.

6.8.4.2 Procedure for one-time or continuous reporting of analytics for user data congestion for a specific UE

The procedure as depicted in Figure 6.8.4.2-1 is used by an NF to retrieve user data congestion analytics for a specific UE. The procedure can be used to request a one-time or continuous reporting of user data congestion analytics.

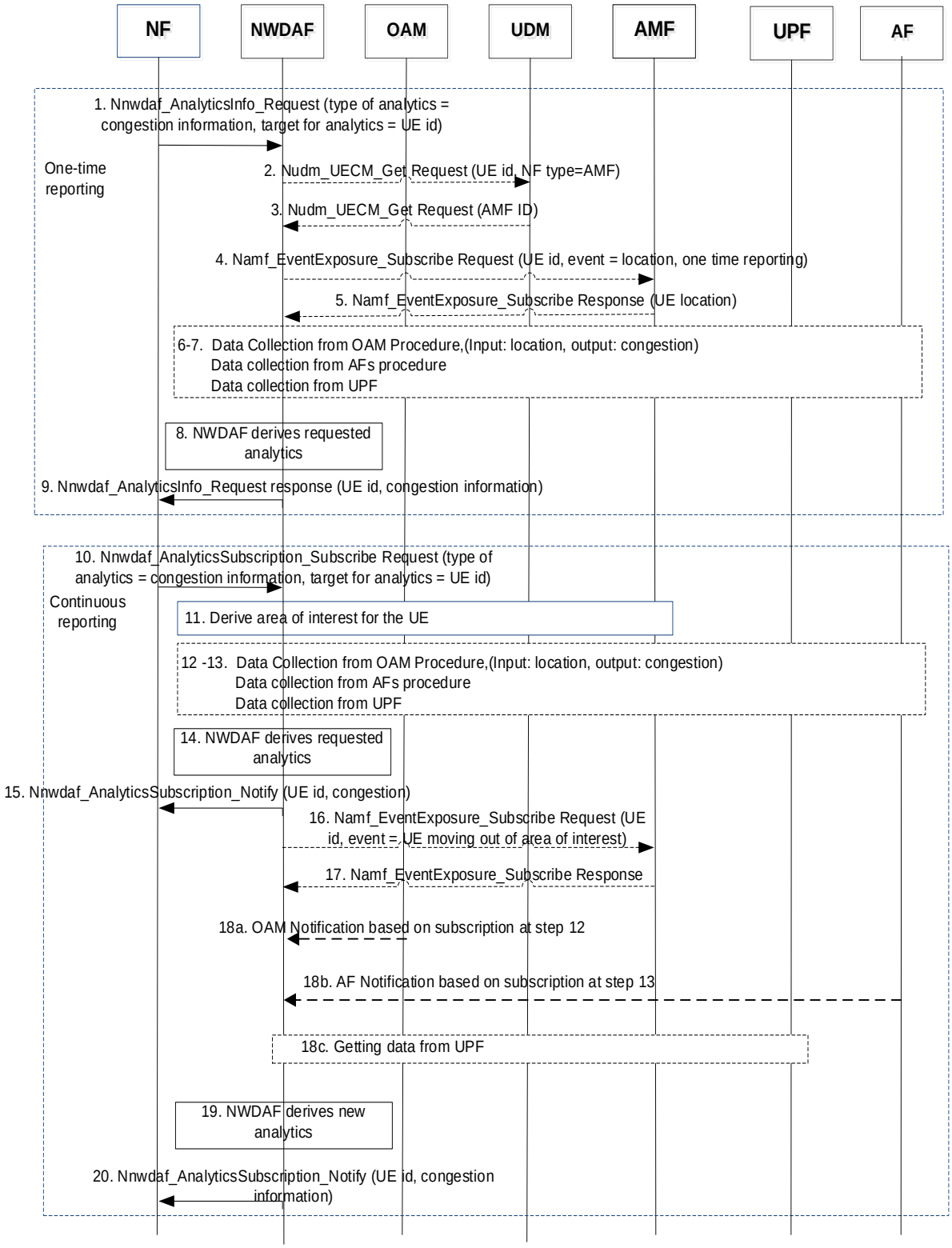

Figure 6.8.4.2-1: Procedure for one-time or continuous reporting of analytics for congestion for a specific UE

For one-time reporting:

1. The NF sends Nnwdaf_AnalyticsInfo_Request to NWDAF, requesting for analytics for user data congestion for a specific UE id. The NF can request statistics or predictions or both. The type of analytics is set to user data

congestion analytics for transfer over user plane, control plane, or both, the Target of Analytics Reporting is set to UE id.

2-5. The NWDAF may already know the UE location. If not, the NWDAF checks the UE location by first retrieving the AMF serving the UE (steps 2-3) and then by interrogating the AMF about the UE location.

NOTE 1: The NF sends a request for a UE that is registered, so that NWDAF can retrieve the UE location.

6-7. The NWDAF requests measurement information for the UE location from OAM services (as captured in 6.2.3.2). These steps are omitted if the NWDAF already has the information. The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

If the request is to provide the list of applications that contribute the most to the traffic, then the NWDAF collects the input data from the UPF serving the UE location, or from the AF(s) by invoking Naf_EventExposure_Subscribe service or Nnef_EventExposure_Subscribe (if via NEF) or collects input data from both, AF and UPF. The input data is defined in Table 6.8.2-2.

8. The NWDAF derives requested analytics.

9. The NWDAF provides the analytics for congestion to the NF.

For continuous reporting:

10. The NF sends Nnwdaf_AnalyticsSubscription_Subscribe Request to the NWDAF. The NF can request for statistics or for predictions or for both. The type of analytics is set to user data congestion analytics for transfer over user plane, control plane, or both.

11. The NWDAF determines the UE location, either via internal information or by applying the same steps as steps 2 to 5. The NWDAF then determines an area of interest.

12-13. The NWDAF subscribes to OAM services (as captured in 6.2.3.2) to get the measurement information for the UE location, possibly providing measurement thresholds. The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

If the request is to provide the list of applications that contribute the most to the traffic, then the NWDAF collects input data from the UPF serving the UE location or from the AF(s) by invoking Naf_EventExposure_Subscribe service or Nnef_EventExposure_Subscribe (if via NEF) or collects from both, AF and UPF. The input data is defined in Table 6.8.2-2.

14. The NWDAF derives requested analytics.

15. The NWDAF provides the analytics for user data congestion status information to the NF.

16-17. The NWDAF subscribes to UE mobility event notification in order to be informed when the UE moves out of the area of interest (in order to define a new area of interest and request new information to OAM if the UE moves to a different area).

18a. A change of user data congestion status corresponding to crossing a threshold set by the NWDAF is detected by OAM and notified to NWDAF.

18b. The AF notifies the NWDAF with the input data as defined in table 6.8.2-2.

18c. The UPF provides the NWDAF with the input data as defined in table 6.8.2-2.

NOTE 2: How NWDAF collects information from UPF is not defined in this Release of the specification.

19. The NWDAF derives new analytics.

20. The NWDAF provides a notification for analytics for the user data congestion status information to the NF.

6.9 QoS Sustainability Analytics

6.9.1 General

The consumer of QoS Sustainability analytics may request the NWDAF analytics information regarding the QoS change statistics for an Analytics target period in the past in a certain area or the likelihood of a QoS change for an Analytics target period in the future in a certain area. The consumer can request either to subscribe to notifications (i.e. a Subscribe-Notify model) or to a single notification (i.e. a Request-Response model).

The service consumer may be a NF (e.g. AF).

The request includes the following parameters:

- Analytics ID = "QoS Sustainability";
- Target of Analytics Reporting: any UE;
- Analytics Filter Information:
  - QoS requirements (mandatory):
    - 5QI (standardized or pre-configured), and applicable additional QoS parameters and the corresponding values (conditional, i.e. it is needed for GBR 5QIs to know the GFBR); or
    - the QoS Characteristics attributes including Resource Type, PDB, PER and their values;
  - Location information (mandatory): an area or a path of interest. The location information could reflect a list of waypoints;

NOTE: In this Release, the consumer of the "QoS Sustainability" Analytics ID will provide location information in the area of interest format (TAIs or Cell IDs) which is understandable by NWDAF.

  - S-NSSAI (optional);
- Optional maximum number of objects;
- Analytics target period: relative time interval, either in the past or in the future, that indicates the time period for which the QoS Sustainability analytics is requested;
- Reporting Threshold(s), which apply only for subscriptions and indicate conditions on the level to be reached for the reporting of the analytics, i.e. to discretize the output analytics and to trigger the notification when the threshold(s) provided in the analytics subscription are crossed by the expected QoS KPIs.
  - A matching direction may be provided such as crossed (default value), below, or above.
  - An acceptable deviation from the threshold level in the non-critical direction (i.e. in which the QoS is improving) may be set to limit the amount of signalling.

    The level(s) relate to value(s) of the QoS KPIs defined in TS 28.554 [10], for the relevant 5QI:

    - for a 5QI of GBR resource type, the Reporting Threshold(s) refer to the QoS flow Retainability KPI;
    - for a 5QI of non-GBR resource type, the Reporting Threshold(s) refer to the RAN UE Throughput KPI.
- In a subscription, the Notification Correlation Id and the Notification Target Address.

The NWDAF collects the corresponding statistics information on the QoS KPI for the relevant 5QI of interests from the OAM, i.e. the QoS flow Retainability or the RAN UE Throughput as defined in TS 28.554 [10].

If the Analytics target period refers to the past:

- The NWDAF verifies whether the triggering conditions for the notification of QoS change statistics are met and if so, generates for the consumer one or more notifications.
- The analytics feedback contains the information on the location and the time for the QoS change statistics and the Reporting Threshold(s) that were crossed.

If the Analytics target period is in the future:

- The NWDAF detects the need for notification about a potential QoS change based on comparing the expected values for the KPI of the target 5QI against the Reporting Threshold(s) provided by the consumer in any cell in the requested area for the requested Analytics target period. The expected KPI values are derived from the statistics for the 5QI obtained from OAM. OAM information may also include planned or unplanned outages detection and other information that is not in scope for 3GPP to discuss in detail.

- The analytics feedback contains the information on the location and the time when a potential QoS change may occur and what Reporting Threshold(s) may be crossed.

6.9.2 Input data

Table 6.9.2-1: Data collection for "QoS Sustainability" analytics

Information	Source	Description
RAN UE Throughput	OAM TS 28.554 [10]	Average UE bitrate in the cell (Payload data volume on RLC level per elapsed time unit on the air interface, for transfers restricted by the air interface), per timeslot, per cell, per 5QI and per S-NSSAI.
QoS flow Retainability	OAM TS 28.554 [10]	Number of abnormally released QoS flows during the time the QoS Flows were used per timeslot, per cell, per 5QI and per S-NSSAI.

NOTE: The timeslot is the time interval split according to the time unit of the OAM statistics defined by operator.

6.9.3 Output analytics

The NWDAF outputs the QoS Sustainability analytics. Depending on the Analytics target period, the output consists of statistics or predictions. The detailed information provided by the NWDAF is defined in Table 6.9.3-1 for statistics and Table 6.9.3-2 for predictions.

Table 6.9.3-1: "QoS Sustainability" statistics

Information	Description
List of QoS sustainability Analytics (1..max)	
>Applicable Area	A list of TAIs or Cell IDs within the Location information that the analytics applies to.
>Applicable Time Period	The time period within the Analytics target period that the analytics applies to.
>Crossed Reporting Threshold(s)	The Reporting Threshold(s) that are met or exceeded or crossed by the statistics value or the expected value of the QoS KPI.

Table 6.9.3-2: "QoS Sustainability" predictions

Information	Description
List of QoS sustainability Analytics (1..max)	
>Applicable Area	A list of TAIs or Cell IDs within the Location information that the analytics applies to.
>Applicable Time Period	The time period within the Analytics target period that the analytics applies to.
>Crossed Reporting Threshold(s)	The Reporting Threshold(s) that are met or exceeded or crossed by the statistics value or the expected value of the QoS KPI.
>Confidence	Confidence of the prediction.

NOTE 1: The meaning of Confidence is based on the SLA, i.e. the consumer has to understand the meaning of the different values of Confidence.

NOTE 2: The Analytics can contain multiple sets of the above information if the location information reflected a list of waypoints.

The number of QoS sustainability analytics entries is limited by the maximum number of objects provided as part of Analytics Reporting Information.

6.9.4 Procedures

Figure 6.9.4-1 depicts a procedure for "QoS Sustainability" analytics provided by NWDAF.

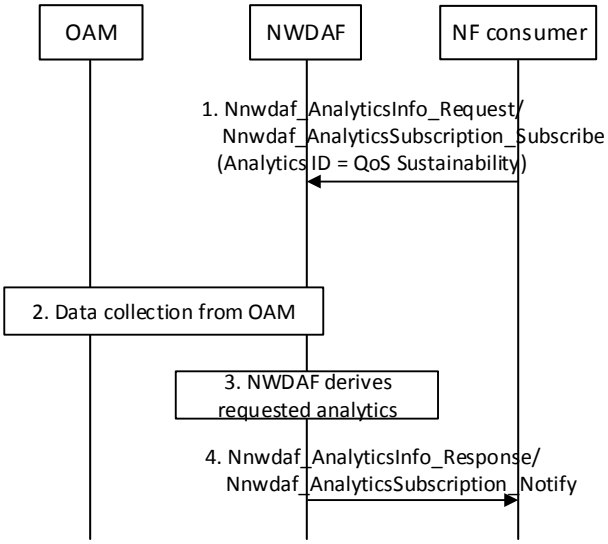

Figure 6.9.4-1: "QoS Sustainability"analytics provided by NWDAF

1. The consumer requests or subscribes to analytics information on "QoS Sustainability" provided by NWDAF. The parameters included in the request are described in clause 6.9.1.

   The consumer may include multiple sets of parameters in order to provide different combinations of "Location information" and "Analytics target period" when requesting QoS Sustainability analytics.

2. The NWDAF collects the data specified in clause 6.9.2 from the OAM, following the procedure captured in clause 6.2.3.2.

3. The NWDAF verifies whether the triggering conditions are met and derives the requested analytics. The NWDAF can detect the need for notification based on comparing the requested analytics of the target 5QI against the Reporting Threshold(s) provided by consumer in any cell over the requested Analytics target period.

4. The NWDAF provides response or notification on "QoS Sustainability" to the consumer.

6.10 Dispersion Analytics

6.10.1 General

Dispersion analytics identifies the location (i.e. areas of interest, TAs, cells) or network slice(s) where a UE, or a group of UEs, or any UE disperse most (if not all) of their data volume and sessions transactions (i.e. MM and SM messages).

The NWDAF shall be able to provide dispersion statistics or predictions and shall be able to collect UE dispersion related information from NFs.

Dispersion is the percentage of activity that a UE, or group of UEs, or any UE, generates at a location or a slice during a period of interest. This enables the operator to rank hot locations or slices by the various activities and to identify the top contributors (i.e. UEs) for that activity. When heavy UEs at a particular location or slice are detected/predicted and reported to a policy entity, their QoS attributes, or access to an area of interest or a slice can then be limited.

- Data volume dispersion - The percentage of data traffic volume that a UE, or a group of UEs, or any UE, generated at a location or in a slice during the period of interest.

- Transactions dispersion - The percentage of MM and SM messages that a UE, or a group of UEs, or any UE, generated at a location or in a slice during the period of interest.

The operator may classify and assign one of the three mobility classes per dispersion characteristics for a UE or a group of UEs, or any UE as fixed, camper or traveller. In addition, the operator may classify a UE as a Top-Heavy UE in case its dispersion percentile rating, at a location or a slice, is higher than a threshold value defined by the operator (e.g. 0.9 percentile), see percentile ranking in the output tables, clause 6.10.3. The classification is based on either Data volume dispersion or Transactions dispersion.

- Data-Classification - fixed, camper, traveller data-classification per thresholds assigned by the operator.

EXAMPLE: When a UE disperses, during the period of observation, most (threshold=95%) of its data at a location or a slice, the dispersion data-classification of the UE at that location or slice is "fixed".

- Transaction-Classification - fixed, camper, traveller transactions-classifications per thresholds assigned by the operator.

EXAMPLE: When a UE disperses, during the period of observation, (threshold=40%) of its session transactions at a location or a slice, the dispersion transaction-classification of the UE is camper at that location or slice.

Based on the dispersion analytics, the analytics consumer can determine that a data volume or transactions hot spot is formed when the volume of data or amount of transactions dispersed by most of the UEs at the area of interest or slice exceeds a certain data or transaction threshold established through trend analysis or operator policy.

The consumer of dispersion analytics may indicate in its request:

- Analytics ID = "Dispersion Analytics";

- Target of Analytics Reporting: a single UE (SUPI), or a group of UEs (an Internal Group ID), or any UE. "Any UE" is only supported in combination with Analytics Filter Information (S-NSSAI, Area(s) of Interest, Top-Heavy UEs indication, Fixed indication, Camper indication or Traveller indication) and Dispersion Analytics type "Data Volume Dispersion Analytics";

- Analytics Filter Information:

  - optional list of TA(s), Area(s) of Interest, Cells, or S-NSSAI(s), Application ID(s), Top-Heavy UEs, Fixed UEs, Camper UEs, Dispersion Analytics type (Data Volume Dispersion Analytics (DVDA) or Transactions Dispersion Analytics (TDA) or both); and

  - optional list of analytics subsets that are requested (see clause 6.10.3);

- Preferred level of accuracy of the analytics;

- Preferred level of accuracy per analytics subset (see clause 6.10.3);

- Preferred order of results for the list of UE Dispersion Analytics information:

  - ordering criterion:

    - For DDA, one of the following: "time slot start", "data dispersion", "data classification", "data ranking", or "data percentile ranking";

    - For TDA, one of the following: "time slot start", "transaction dispersion", "transaction classification", "transaction ranking", or "transaction percentile ranking"; and

  - order: ascending or descending;

- Analytics target period indicating the time period over which the statistics or predictions are requested;

- Optionally, maximum number of objects and maximum number of SUPIs;

- Optionally, preferred granularity of location information: TA level or cell level; and

- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

NOTE 1: If one or multiple ID(s) are included in the filter information, the output analytics will be reported per Application ID, otherwise the output analytics is aggregated information per AOI or slice independent of the applications.

NOTE 2: Care needs to be taken with regards to load when requesting analytics for "Any UE". This could be achieved by utilizing event filters (e.g. Area of Interest for AMF) and possible analytics filters including Top-Heavy UEs, and/or Fixed and/or Camper UEs and/or Analytics Reporting Information (e.g. SUPImax), or sampling ratio as part of Event Reporting Information. The load of analytics for "Any UE" can be alleviated by limiting the number of S-NSSAI in the analytics filter.

6.10.2 Input Data

The NWDAF shall be able to collect UE dispersion information from NF(s) and AFs. The information collected by the NWDAF is network data from 5GC NFs and service data from AFs:

- Data related to UE transactions dispersion and bound by location collected from AMF and SMF are defined in the tables 6.10.2-1 and 6.10.2-2. This may include individual transactions or SMF/AMF state transition information stored as UE behaviour trends, which provides aggregated transaction information.

Table 6.10.2-1: Location based UE transactions dispersion information collected from serving AMF

Information	Source	Description
UE ID	AMF	SUPI.
Type Allocation Code	AMF	Terminal model and vendor information of the UE.
UE locations (1..max)	AMF	UE locations.
>UE location	AMF	Area of Interest (TA or cells that the UE had entered).
>Timestamp	AMF	Time stamp when the AMF detected that the UE had entered this location.
>Transactions	AMF	Either all transactions for this UE in this location or, optionally, if subscription with periodic notification is requested,the amount of UE transactions exchanged at the location in the notified time period.
UE access behaviour trends	AMF	Metrics on UE state transitions (e.g., access, RM and CM states, handover).
UE location trends	AMF	Metrics on UE locations.
NOTE: UE location provides one location per instance while UE location trend provides multiple locations at once. One or both of them may be used.		

Table 6.10.2-2: UE transactions dispersion information collected from serving SMF

Information	Source	Description
UE IP address	SMF	UE IP address.
UE ID	SMF	SUPI.
>Timestamp	SMF	Time stamp of the collected information.
>Transactions	SMF	Either all transaction for this UE or, optionally, if subscription with periodic notification is requested,the amount of UE transactions exchanged in the notified time period.
> UE session behaviour trends	SMF	Metrics on UE state transitions (e.g. PDU Session Establishment, PDU Session Release).

Data volume can be collected from the AF per UE across all the UE applications provided by a particular AF or per UE per application when application IDs are requested.

Data related to UE data volume dispersion, bound by a location or slice, collected from the AF and UPF are defined in tables 6.10.2-3 through 6.10.2-6.

If the Target of Analytics Reporting is set to an Internal Group ID and the AF is located in the untrusted domain, NEF translates it into an External Group ID.

NOTE 1: It is assumed that the AF is provisioned with the list of UE IDs (GPSIs or SUPIs) belonging to an External or Internal Group ID.

- In table 6.10.2-3, the data volume is collected per UE from the AF. The collected UE information is applicable across all the applications used by the UE during the period.

Table 6.10.2-3: UE Data volume dispersion information collected from the AF

Information	Source	Description
UE ID	AF	Internal or External UE ID (i.e. SUPI or GPSI, respectively).
Timestamp	AF	Time stamp of the collected information.
>Data Volume UL/DL	AF	Sum of UE data volume exchanged at the AF during the period of observation.

- In table 6.10.2-4, the AF reports data volume per UE per application in relation to the start and stop of the application as indicated by the application duration.

Table 6.10.2-4: UE data volume dispersion collected from the AF

Information	Source	Description
UE IP address	AF	UE IP address.
IP 5-tuple	AF	IP address 5-tuple.
Timestamp	AF	Timestamp of the collected information.
Application ID	AF	Identifier of the application at the AF.
Location of Application	AF/NEF	Location of application represented by a list of DNAI(s). The NEF may map the AF-Service identifier information to a list of DNAI(s) when the DNAI(s) being used by the application are statically defined.
Data Volume UL/DL	AF	Sum of UE data volume exchanged per application during the period.
Application duration	AF	Duration for the application (e.g. Voice talk time).
NOTE 1: Application ID and IP 5-tuple are mutually exclusive. NOTE 2: Multiple outputs are provided by the AF when multiple applications are running at the AF for the same UE and time period.		

Data volume can also be collected from the UPF per UE IP address across all applications or per UE for specific application(s).

- In table 6.10.2-5, the data volume is collected per UE from the UPF. The collected UE information is applicable across all applications used by the UE between start and stop of the PDU session. The UPF reports volume per UE IP address across all applications.

Table 6.10.2-5: UE data volume dispersion collected from serving UPF

Information	Source	Description
UE IP address	UPF	UE IP address.
Timestamp	UPF	Time stamp of the collected information.
Data Volume UL/DL	UPF	Sum of UE data volume exchanged per UE across all applications.
NOTE: The Data volume can be reported either as total volume of the PDU session or periodically. It refers to the Data volume exchanged between the start and stop of the PDU session. When reported periodically, the period can be specified in the requested analytic target period or configured as a default value in the UPF.		

- In table 6.10.2-6, the UPF reports data volume per UE for specific application(s) in relation to the start and stop of the application as indicated by the application duration.

There are two modes of data collection:

- Non periodical: A mode where the data volume is requested and consequently provided for the total volume of a PDU session.

- Periodical: A mode where data volume is provided periodically between the start and stop of a PDU session. The period can be specified in the requested analytic target period or configured as a default value in the UPF.

For both modes of data collection, if there are multiple application sessions for the UE PDU session, the NWDAF aggregates (i.e. sums up) the data volume across all applications to obtain per UE information.

Table 6.10.2-6: UE data volume dispersion collected from serving UPF

Information	Source	Description
UE IP address	UPF	UE IP address.
Timestamp	UPF	A timestamp of the collected information.
Application ID	UPF	Identify the application at the UPF
IP 5-tuple	UPF	IP 5-tuple.
Location of Application	UPF	List of Internet applications represented by DNAI(s).
Data Volume UL/DL	UPF	Sum of UE data volume exchanged per application during the period.
Application duration	UPF	Duration for the application (e.g. Voice talk time).
NOTE 1: Application ID and IP 5-tuple are mutually exclusive. NOTE 2: Multiple outputs are provided by the UPF when multiple applications are running at the UPF for the same UE and time period. NOTE 3: The Data volume can be reported either as total volume of the PDU session or periodically. It refers to the Data volume exchanged between the start and stop of the PDU session. When reported periodically, the period can be specified in the requested analytic target period or configured as a default value in the UPF.		

The task of the NWDAF is to calculate the volume of data and amount of transactions dispersed by the UE at each visited location during a period of interest. The entry time and exit time to a location is provided by the AMF.

Collecting volume per UE and per specific application is optional and such information can be provided by the UPF or AF.

The Correlation Information as defined in table 6.2.4-1 is used to correlate the input data from AMF and SMF, the input data from SMF and UPF, and the input data from UPF and AF.

- Slice information related to UE transactions dispersion from NF(s) are defined in tables 6.10.2-7 and 6.10.2-8. This may include individual transactions or SMF/AMF state transition information stored as UE behaviour trends, which provides aggregated transaction information.

- The Slice data volume collection is the same as listed in tables 6.10.2-3 to 6.10.2-6.

Table 6.10.2-7: Slice based UE transactions dispersion information collected from serving AMF

Information	Source	Description
UE ID	AMF	SUPI.
Type Allocation Code	AMF	Terminal model and vendor information of the UE.
Slice (1..max)	AMF	UE assigned slice.
>S-NSSAI	AMF	Identifier of the slice.
>Timestamp	AMF	Time stamp when the slice was assigned.
>Transactions (NOTE)	AMF	Either all transactions for this UE or, optionally, if subscription with periodic notification is requested, an amount of UE transactions exchanged at the slice in the notified time period.
UE access behaviour trends	AMF	Metrics on UE state transitions (e.g., access, RM and CM states, handover).
NOTE: When a UE moves to a new AMF during Analytics target period, timestamps for assigned slices of the UE are set to the date and time of the new AMF. The NWDAF shall aggregate (sum up) the amount of slice transactions, for the requested Analytics target period, across the AMFs traversed by the UE.		

Table 6.10.2-8: Slice based UE transactions dispersion information collected from serving SMF

Information	Source	Description
UE IP	SMF	UE IP address.
UE ID	SMF	SUPI.
Slice (1..max)	SMF	UE assigned slice.
>S-NSSAI	SMF	Identifier of the slice.
>Timestamp	SMF	Time stamp associated with the collected information.
>Application ID	SMF	Identifier of the application for the UE in the slice.
>Transactions	SMF	Either all transactions for this UE or, optionally, if subscription with periodic notification is requested, an amount of UE transactions exchanged at the slice in the notified time period.
UE session behaviour trends	SMF	Metrics on UE state transitions (e.g. PDU Session Establishment, PDU Session Release).

The task of the NWDAF is to calculate the volume of data and amount of transactions dispersed by the UE at each slice during a period of interest. A time stamp of a slice assignment is provided by the AMF.

The Correlation Information as defined in table 6.2.4-1 is used to correlate the input data from AMF and SMF, the input data from SMF and UPF, and the input data from UPF and AF.

Data collection may be provided on samples (e.g. spatial subsets of UEs or UE group, temporal subsets of UE location information).

NOTE 2: How the data from UPF is retrieved is not specified in this release.

NOTE 3: The list of monitored transactions (MM and SM messages) is a subset of the messages listed in clauses 8.2 and 8.3 of TS 24.501 [23].

NOTE 4: The Namf_EventExposure and Nsmf_EventExposure services in clauses 5.2.2.3 and 5.2.8.3 of TS 23.502 [3] provide the required transactions information.

6.10.3 Output Analytics

6.10.3.0 General

The NWDAF provides UE dispersion analytics, which can be statistics and/or prediction for data volume and/or transactions dispersions, to consumer NFs or AFs.

6.10.3.1 Data Volume Dispersion Analytics

The data volume dispersion analytics results provided by the NWDAF can be for a UE or group of UEs or "any UE" data volume dispersion statistics as defined in table 6.10.3.1-1 and/or UE data volume dispersion predictions as defined in table 6.10.3.1-2. If the analytics covers multiple UEs, the Data dispersed, Data ranking, and Data percentile ranking parameters are calculated as the aggregated (i.e. summed up) data volume. When the Target of Analytics Reporting is set as "any UE" the data volume dispersion analytics results provided by the NWDAF can be for all UEs data volume dispersion statistics at a location and/or the slice and/or data volume dispersion predictions at a location and/or the slice.

Table 6.10.3.1-1: Data volume dispersion statistics bound by location

Information	Description
UE group ID or UE ID or list of UE IDs (1..SUPImax)	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or a list of UEs for which the statistic applies (see NOTE 1).
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> UE location (1..max)	Observed location statistics.
>> UE location	TA or cells where the UE or UE group or list of UEs dispersed its data (see NOTE 3).
>> Application ID (0..max) (NOTE 7)	To identify the application (NOTE 6).
>>> Data volume dispersed (NOTE 4)	Data volume dispersed at this location.
>> Data mobility classification (NOTE 4)	Data mobility classification of the UE for this location: fixed, camper, traveller (see NOTE 5).
>> Data usage ranking (NOTE 4) (NOTE 7)	Ranking of UE data usage at this location (See NOTE 2).
>> Datausage percentile ranking (NOTE 4) (NOTE 7)	Percentile ranking of the UE or UE group in the Cumulative Distribution Function of data usage for the population of all UEs served at the location.
>> Ratio	Percentage of UEs in the group at the location and observation time (in the case of UE group).

NOTE 1: When Target of Analytics Reporting is an individual UE, a single UE ID (i.e. SUPI) will be included. When Target of Analytics Reporting is a UE group ID, an internal group ID will be included. When Target of Analytics Reporting is a UE group ID or "Any UE" and a filter for Top-Heavy UEs, fixed, camper or traveller is included, the NWDAF will include the list of UEs matching the filter. This information element is not present when Target of Analytic Reporting is "Any UE" and no filter for Top-Heavy UEs, fixed, camper or traveller is included. The NWDAF will provide the dispersion analytics result of one or a list of time slots to the service consumer(s) for the UE, group of UEs or list of UEs.

NOTE 2: UE is ranked high (i.e. 1), medium (2) and low (3) when its data dispersed, during the period of observation at the location, is higher than N1% or at the range of N1% to N2% or less than N2%, respectively. The percentage values of N1 and N2 are subject to operator's configuration.

NOTE 3: When possible and applicable to the access type, UE location is provided according to the preferred granularity of location information.

NOTE 4: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".

NOTE 5: This parameter is only provided for Target of Analytics Reporting set to single UE.

NOTE 6: When Application ID is not included in the input, cardinality is zero and data volume dispersed is provided per UE location and applies across all the applications in that location.

NOTE 7: This parameter is not provided for Target of Analytics Reporting set to "Any UE".

Table 6.10.3.1-2: Data volume dispersion prediction bound by location

Information	Description
UE group ID or UE ID or list of UE IDs (1..SUPImax)	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or a list of UEs for which the prediction applies (see NOTE 1).
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> UE location (1..max)	Predicted location during the analytics target period.
>> UE location	TA or cells where the UE or UE group or list of UEs is predicted to disperse its data (see NOTE 3).
>> Application ID (0..max) (NOTE 7)	To identify the application (NOTE 6).
>>> Data volume dispersion (NOTE 4)	Data volume dispersion prediction at this location.
>>>> Confidence	Confidence of this prediction (i.e. data volume to be dispersed at this location).
>> Data mobility classification (NOTE 4)	Data mobility classification of the UE for this location: fixed, camper, traveller (see NOTE 5).
>>> Confidence	Confidence of this prediction (i.e. mobility classification at this location).
>> Data usage ranking (NOTE 4) (NOTE 7)	Ranking of UE data usage at this location (See NOTE 2).
>> Data percentileusage ranking (NOTE 4) (NOTE 7)	Percentile ranking of the UE or UE group in the Cumulative Distribution Function of data usage for the population of all UEs served at the location.
>>> Confidence	Confidence of this prediction (i.e. percentile ranking at this location).
>> Ratio	Percentage of UEs in the group (in the case of UE group).

NOTE 1: When Target of Analytics Reporting is an individual UE, a single UE ID (i.e. SUPI) will be included. When Target of Analytics Reporting is a UE group ID, an internal group ID will be included. When Target of Analytics Reporting is a UE group ID or "Any UE" and a filter for Top-Heavy UEs, fixed, camper or traveller is included, the NWDAF will include the list of UEs matching the filter. This information element is not present when Target of Analytic Reporting is "Any UE" and no filter for Top-Heavy UEs, fixed, camper or traveller is included. The NWDAF will provide the dispersion analytics result of one or a list of time slots to the service consumer(s) for the UE, group of UEs or list of UEs.

NOTE 2: UE is ranked high (i.e. 1), medium (2) and low (3) when its data dispersed, during the period of observation at the location, is higher than N1% or at the range of N1% to N2% or less than N2%, respectively. The percentage values of N1 and N2 are subject to operator's configuration.

NOTE 3: When possible and applicable to the access type, UE location is provided according to the preferred granularity of location information.

NOTE 4: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".

NOTE 5: This parameter is only provided for Target of Analytics Reporting set to single UE.

NOTE 6: When Application ID is not included in the input, cardinality is zero and data volume dispersion prediction is provided per UE location and applies across all the applications in that location.

NOTE 7: This parameter is not provided for Target of Analytics Reporting set to "Any UE".

The data volume dispersion analytics results provided by the NWDAF can also be for a UE or group of UEs or "any UE" data volume dispersion statistics at a given slice as defined in Table 6.10.3.1-3 and/or data volume dispersion predictions as defined in Table 6.10.3.1-4. If the analytics covers multiple UEs, the Data dispersed, Data ranking, and Data percentile ranking parameters are calculated as the aggregated (i.e. summed up) data volume. When the Target of Analytics Reporting is set as "any UE" the data volume dispersion analytics results provided by the NWDAF can be for all UEs data volume dispersion statistics at a given slice and/or data volume dispersion predictions at a given slice.

Table 6.10.3.1-3: Data volume dispersion statistics bound by slice

Information	Description
UE group ID or UE ID or a list of UE IDs (1..SUPImax)	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or a list of UEs for which the statistic applies (see NOTE 1).
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> Slice (1..max)	Observed slice statistics.
>> S-NSSAI	Slice where the UE or group of UEs or list of UEs dispersed data.
>> Application ID (0..max) (NOTE 6)	To identify the application at the slice (NOTE 5).
>>> Data volume dispersed (NOTE 3)	Data volume dispersed at this slice.
>> Data mobility classification (NOTE 3)	Data mobility classification of the UE at the slice: fixed, camper, traveller (see NOTE 4).
>> Data usage ranking (NOTE 3) (NOTE 6)	Ranking of UE data usage at this slice. (See NOTE 2).
>> Datausage percentile ranking (NOTE 3) (NOTE 6)	Percentile ranking of the UE or UE group in the Cumulative Distribution Function of data usage for the population of all UEs served by the slice.
>> Ratio	Percentage of UEs in the group (in the case of UE group).

NOTE 1: When Target of Analytics Reporting is an individual UE, a single UE ID (i.e. SUPI) will be included. When Target of Analytics Reporting is a UE group ID, an internal group ID will be included. When Target of Analytics Reporting is a UE group ID or "Any UE" and a filter for Top-Heavy UEs, fixed, camper or traveller is included, the NWDAF will include the list of UEs matching the filter. This information element is not present when Target of Analytic Reporting is "Any UE" and no filter for Top-Heavy UEs, fixed, camper or traveller is included. The NWDAF will provide the dispersion analytics result of one or a list of time slots to the service consumer(s) for the UE, the group of UEs or the list of UEs.

NOTE 2: UE is ranked high (i.e. 1), medium (2) and low (3) when its data dispersed, during the period of observation at the location, is higher than N1% or at the range of N1% to N2% or less than N2%, respectively. The percentage values of N1 and N2 are subject to operator's configuration.

NOTE 3: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".

NOTE 4: This parameter is only provided for Target of Analytics Reporting set to single UE.

NOTE 5: When Application ID is not included in the input, cardinality is zero and data volume dispersed is provided per slice and applies across all the applications in the slice.

NOTE 6: This parameter is not provided for Target of Analytics Reporting set to "Any UE".

Table 6.10.3.1-4: Data volume dispersion prediction bound by slice

Information	Description
UE group ID or UE ID or list of UE IDs (1..SUPImax)	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or a list of UEs for which the prediction applies (see NOTE 1).
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> Slice (1..max)	Predicted slice during the Analytics target period.
>> S-NSSAI	Slice where the UE or UE group or list of UEs is predicted to disperse its data.
>> Application ID (0..max) (NOTE 6)	To identify the application at the slice (NOTE 5).
>>> Data volume dispersion (NOTE 3)	Data volume dispersion prediction at this slice.
>>>> Confidence	Confidence of this prediction (i.e. data volume to be dispersed at this slice).
>> Data mobility classification (NOTE 3)	Data mobility classification of the UE at this slice: fixed, camper, traveller (see NOTE 4).
>>> Confidence	Confidence of this prediction (i.e. mobility classification at this slice).
>> Data usage ranking (NOTE 3) (NOTE 6)	Ranking of UE data usage at this slice. See NOTE 2.
>> Datausage percentile ranking (NOTE 3) (NOTE 6)	Percentile ranking of the UE or UE group in the Cumulative Distribution Function of data usage for the population of all UEs served by the slice.
>>> Confidence	Confidence of this prediction (i.e. percentile ranking at this slice).
>> Ratio	Percentage of UEs in the group (in the case of UE group).

NOTE 1: When Target of Analytics Reporting is an individual UE, a single UE ID (i.e. SUPI) will be included. When Target of Analytics Reporting is a UE group ID, an internal group ID will be included. When Target of Analytics Reporting is a UE group ID or "Any UE" and a filter for Top-Heavy UEs, fixed, camper or traveller is included, the NWDAF will include the list of UEs matching the filter. This information element is not present when Target of Analytic Reporting is "Any UE" and no filter for Top-Heavy UEs, fixed, camper or traveller is included. The NWDAF will provide the dispersion analytics result of one or a list of time slots to the service consumer(s) for the UE, group of UEs or list of UEs.
NOTE 2: UE is ranked high (i.e. 1), medium (2) and low (3) when its data dispersed, during the period of observation at the location, is higher than N1% or at the range of N1% to N2% or less than N2%, respectively. The percentage values of N1 and N2 are subject to operator's configuration.
NOTE 3: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".
NOTE 4: This parameter is only provided for Target of Analytics Reporting set to single UE.
NOTE 5: When Application ID is not included in the input, cardinality is zero and data volume dispersion prediction is provided per slice and applies across all the applications in the slice.
NOTE 6: This parameter is not provided for Target of Analytics Reporting set to "Any UE".

When the Target of Analytics Reporting is set as "any UE", no filter for Top-Heavy UEs, fixed, camper or traveller is included and the Analytics Filter Information is set to one or several S-NSSAIs and DDVA, the data volume dispersion analytics results provided by the NWDAF can be for all UEs data volume dispersion statistics at a given slice as defined in Table 6.10.3.1-5 and/or data volume dispersion predictions as defined in Table 6.10.3.1-6:

Table 6.10.3.1-5: Data volume dispersion statistics bound by slice (for any UE)

Information	Description
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> Slice (1..max)	Observed slice statistics.
>> S-NSSAI	Slice where all UEs dispersed data.
>> Data volume dispersed	Data volume dispersed at this slice. (see NOTE 1).

NOTE 1: Utilized bandwidth (i.e. average throughput) at the slice can be calculated by using the Data volume dispersed in the Duration.

Table 6.10.3.1-6: Data volume dispersion prediction bound by slice (for any UE)

Information	Description
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> Slice (1..max)	Predicted slice during the Analytics target period.
>> S-NSSAI	Slice where the UE is predicted to disperse its data.
>> Data volume dispersion	Data volume dispersion prediction at this slice. (see NOTE 1).
>>>> Confidence	Confidence of this prediction (i.e. data to be dispersed at this slice).
NOTE 1: Utilized bandwidth (i.e. average throughput) predication at the slice can be calculated by using the Data volume dispersion in the Duration.	

NOTE: The Application ID in the Data Volume Dispersion Analytics is optional. When the Application ID is missing, the Data Volume Dispersion Analytics is applied across all the applications in an AOI or a slice.

6.10.3.2 Transactions Dispersion Analytics

The transactions (MM and MS messages) dispersion analytics results provided by the NWDAF can be for a UE or group of UEs transactions dispersion statistics as defined in Table 6.10.3.2-1 and/or UE transactions dispersion predications as defined in Table 6.10.3.2-2. If the analytics covers multiple UEs, the Transactions dispersed, Transactions ranking, and Transactions percentile ranking parameters are calculated as the aggregated (i.e. summed up) number of transactions.

Table 6.10.3.2-1: Transactions dispersion statistics bound by location

Information	Description
UE group ID or UE ID or list of UE IDs (1..SUPImax)	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or a list of UEs for which the statistic applies (see NOTE 1).
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> UE location (1..max)	Observed location statistics.
>> UE location	TA or cells where the UE or group of UEs or list of UEs dispersed its transactions (see NOTE 3).
>> Transactions dispersed (NOTE 4)	Transactions amount dispersed at this location.
>> Transactions mobility classification (NOTE 4)	Transactions mobility classification of the UE for this location: fixed, camper, traveller (see NOTE 5).
>> Transactions ranking (NOTE 4)	Ranking of transactions amount at this location.See NOTE 2.
>> Transactions percentile ranking (NOTE 4)	Percentile ranking of the UE or UE group in the Cumulative Distribution Function of transactions for the population of all UEs served at the location.
>> Ratio	Percentage of UEs in the group (in the case of UE group).
NOTE 1: When Target of Analytics Reporting is an individual UE, a single UE ID (i.e. SUPI) will be included. When Target of Analytics Reporting is a UE group ID, an internal group ID will be included. When Target of Analytics Reporting is a UE group ID and a filter for Top-Heavy UEs, fixed, camper or traveller is included, the NWDAF will include the list of UEs matching the filter. The NWDAF will provide the dispersion analytics result of one or a list of time slots to the service consumer(s) for the UE, group of UEs or list of UEs. NOTE 2: UE is ranked high (i.e. 1), medium (2) and low (3) when its transactions are dispersed, during the period of observation at the location, is higher than N1% or at the range of N1% to N2% or less than N2%, respectively. The percentage values of N1 and N2 are subject to operator's configuration. NOTE 3: When possible and applicable to the access type, UE location is provided according to the preferred granularity of location information. NOTE 4: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset". NOTE 5: This parameter is only provided for Target of Analytics Reporting set to single UE.	

Table 6.10.3.2-2: Transactions dispersion prediction bound by location

Information	Description
UE group ID or UE ID or list of UE IDs (1..SUPImax)	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or a list of UEs for which the prediction applies (see NOTE 1).
Time slot entry (1..max)	List of predicted time slots.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> UE location (1..max)	Predicted location during the analytic target period.
>> UE location	TA or cells where the UE or group of UEs or list of UEs is predicted to disperse its transactions (see NOTE 3).
>> Transactions dispersion (NOTE 4)	Transaction amount predicted to be dispersed at this location.
>>> Confidence	Confidence of this prediction (i.e. data to be dispersed at this location).
>> Transactions mobility classification (NOTE 4)	Transaction mobility classification of the UE for this location: fixed, camper, traveller (see NOTE 5).
>>> Confidence	Confidence of this prediction (i.e. mobility classification at this location).
>> Transactions ranking (NOTE 4)	Ranking of transactions amount at this location. See NOTE 2.
>> Transactions percentile ranking (NOTE 4)	Percentile ranking of the UE or UE group in the Cumulative Distribution Function of transactions for the population of all UEs served at the location.
>>> Confidence	Confidence of this prediction (i.e. percentile ranking at this location).
>> Ratio	Percentage of UEs in the group (in the case of UE group).

NOTE 1: When Target of Analytics Reporting is an individual UE, a single UE ID (i.e. SUPI) will be included. When Target of Analytics Reporting is a UE group ID, an internal group ID will be included. When Target of Analytics Reporting is a UE group ID and a filter for Top-Heavy UEs, fixed, camper or traveller is included, the NWDAF will include the list of UEs matching the filter. The NWDAF will provide the dispersion analytics result of one or a list of time slots to the service consumer(s) for the UE, group of UEs or list of UEs.

NOTE 2: UE is ranked high (i.e. 1), medium (2) and low (3) when its transactions are dispersed, during the period of observation at the location, is higher than N1% or at the range of N1% to N2% or less than N2%, respectively. The percentage values of N1 and N2 are subject to operator's configuration.

NOTE 3: When possible and applicable to the access type, UE location is provided according to the preferred granularity of location information.

NOTE 4: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".

NOTE 5: This parameter is only provided for Target of Analytics Reporting set to single UE.

The transactions dispersion analytics results provided by the NWDAF can be UE or group of UEs transactions dispersion statistics at a given slice as defined in table 6.10.3.2-3 and/or transactions dispersion predictions as defined in table 6.10.1.4.2-4. If the analytics covers multiple UEs, the Transactions dispersed, Transactions ranking, and Transactions percentile ranking parameters are calculated as the aggregated (i.e. summed up) number of transactions.

Table 6.10.3.2-3: Transactions dispersion statistics bound by slice

Information	Description
UE group ID or UE ID or a list of UE IDs (1..SUPImax)	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or a list of UEs for which the statistic applies (see NOTE 1).
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> Slice (1..max)	Observed slice statistics.
>> S-NSSAI	Slice where the UE or group of UEs or list of UEs dispersed its transactions.
>> Transactions dispersed (NOTE 3)	Transactions amount dispersed at this location.
>> Transactions mobility classification (NOTE 3)	Transaction mobility classification of the UE at the slice: fixed, camper, traveller (see NOTE 4).
>> Transactions ranking (NOTE 3)	Ranking of transactions amount at this slice. See NOTE 2.
>> Transactions percentile ranking (NOTE 3)	Percentile ranking of the UE or UE group in the Cumulative Distribution Function of transactions for the population of all UEs served by the slice.
>> Ratio	Percentage of UEs in the group (in the case of UE group).

NOTE 1: When Target of Analytics Reporting is an individual UE, a single UE ID (i.e. SUPI) will be included. When Target of Analytics Reporting is a UE group ID, an internal group ID will be included. When Target of Analytics Reporting is a UE group ID and a filter for Top-Heavy UEs, fixed, camper or traveller is included, the NWDAF will include the list of UEs matching the filter. The NWDAF will provide the dispersion analytics result of one or a list of time slots to the service consumer(s) for the UE, the group of UEs or the list of UEs.

NOTE 2: UE is ranked high (i.e. 1), medium (2) and low (3) when its transactions are dispersed, during the period of observation at the location, is higher than N1% or at the range of N1% to N2% or less than N2%, respectively. The percentage values of N1 and N2 are subject to operator's configuration.

NOTE 3: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".

NOTE 4: This parameter is only provided for Target of Analytics Reporting set to single UE.

Table 6.10.3.2-4: Transactions dispersion prediction bound by slice

Information	Description
UE group ID or UE ID or list of UE IDs (1..SUPImax)	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or a list of UEs for which the prediction applies (see NOTE 1).
Time slot entry (1..max)	List of predicted time slots.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot.
> Slice (1..max)	Predicted slice during the Analytics target period.
>> S-NSSAI	Slice where the UE or group of UEs or list of UEs is predicted to disperse its transactions.
>> Transactions dispersion (NOTE 3)	Transaction volume to be dispersed at this slice.
>>> Confidence	Confidence of this prediction (i.e. transactions to be dispersed at this slice).
>> Transactions mobility classification (NOTE 3)	Transaction mobility classification of the UE at this slice: fixed, camper, traveller (see NOTE 4).
>>> Confidence	Confidence of this prediction (i.e. mobility classification at this slice).
>> Transactions ranking (NOTE 3)	Ranking of transactions amount at this slice. See NOTE 2.
>> Transactions percentile ranking (NOTE 3)	Percentile ranking of the UE or UE group in the Cumulative Distribution Function of transactions for the population of all UEs served by the slice.
>>> Confidence	Confidence of this prediction (i.e. percentile ranking at this slice).
>> Ratio	Percentage of UEs in the group (in the case of UE group).

NOTE 1: When Target of Analytics Reporting is an individual UE, a single UE ID (i.e. SUPI) will be included. When Target of Analytics Reporting is a UE group ID an internal group ID will be included. When Target of Analytics Reporting is a UE group ID and a filter for Top-Heavy UEs, fixed, camper or traveller is included, the NWDAF will include the list of UEs matching the filter. The NWDAF will provide the dispersion analytics result of one or a list of time slots to the service consumer(s) for the UE, group of UEs or list of UEs.

NOTE 2: UE is ranked high (i.e. 1), medium (2) and low (3) when its transactions are dispersed, during the period of observation at the location, is higher than N1% or at the range of N1% to N2% or less than N2%, respectively. The percentage values of N1 and N2 are subject to operator's configuration.

NOTE 3: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".

NOTE 4: This parameter is only provided for Target of Analytics Reporting set to single UE.

6.10.4 Dispersion Analytic Procedure

The NWDAF can provide Dispersion analytics, in the form of statistics or predictions, to an NF or AF.

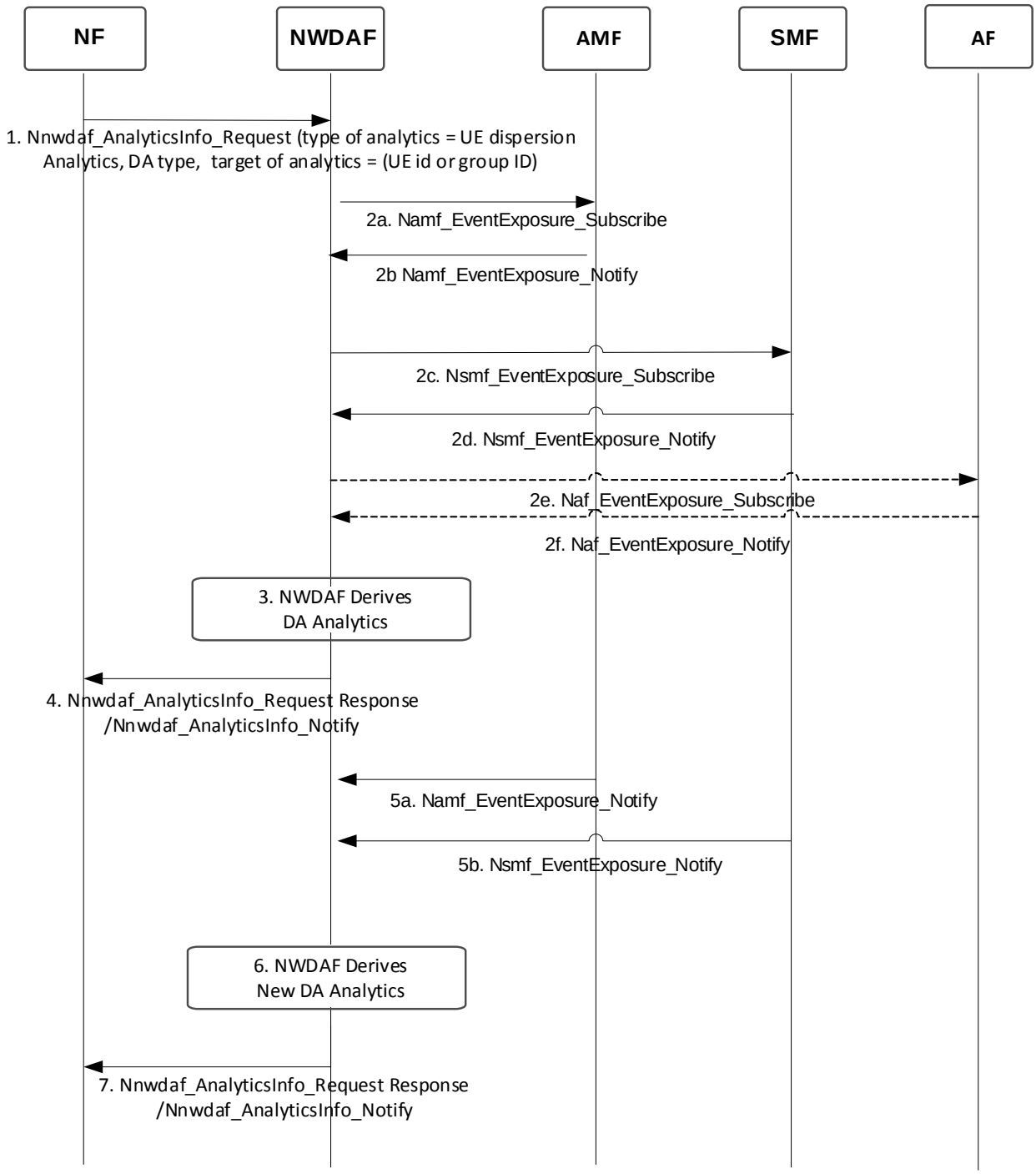

Figure 6.10.4-1: UE Dispersion Analytics provided to an NF or AF

1. The NF sends a request to the NWDAF for dispersion analytics on a specific UE, any UE, or a group of UEs, using either the Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription service. The NF can request statistics or predictions or both. The Analytics ID is set to "UE Dispersion Analytics", the Dispersion Analytic (DA) type is set to "Data Volume Dispersion Analytics" (DVDA) or "Transactions Dispersion Analytics" (TDA) and Analytic Filter Information = (Area of Interest, slice, target period, optional UE class: Top-Heavy, Fixed, or Camper UEs). The NF or AF provides the UE ID or Internal Group ID in the Target of Analytics Reporting.

2. If the request is authorized, and in order to provide the requested analytics, the NWDAF may subscribe to events with all the serving AMFs, SMFs of the requested UE(s) for notification of location changes or a slice change (a slice change can be an additional slice or a deletion), or to obtain UE location trends, UE access behaviour trends and UE session behaviour trends. This stepmay be skipped when, e.g. the NWDAF already has the requested analytics available.

The NWDAF subscribes to application service data from AF(s) by invoking Naf_EventExposure_Subscribe service or Nnef_EventExposure_Subscribe (via NEF).

The NWDAF can collect data volume information from the UPF, as listed in tables 6.10.2-5 and 6.10.2-6 and clause 6.2.2.1, however, how information is collected from UPFs is not defined in this Release of the specification.

NOTE: The NWDAF determines the AMF serving the UE, any UE, or the group of UEs as described in clause 6.2.2.1.

3. The NWDAF derives requested analytics.

4. The NWDAF provides requested UE dispersion analytics to the NF, using either the Nnwdaf_AnalyticsInfo_Request Response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1. The details for UE dispersion analytics provided by NWDAF are described in clause 6.10.3. The provided analytics enables the consumer to predict changing network conditions such as data volume change at a location or a slice, excessive signalling conditions at a location or a slice, etc.

5-6. If at step 1, the NF has subscribed to receive notifications for UE dispersion analytics, after receiving event notification from the AMFs (e.g. location change) or SMFs (e.g. slice change add/delete) subscribed by NWDAF in step 2, the NWDAF may generate new dispersion analytics.

7. The NWDAF provides the newly generated dispersion analytics to the NF. The details for UE dispersion analytics provided by NWDAF are described in clause 6.10.3.

6.11 WLAN performance analytics

6.11.1 General

The NWDAF provides WLAN performance analytics to a service consumer NF. The analytics results are generated based on the data from other 5GC NFs and OAM. The analytics results, provided in the form of statistics or predictions, contain quality and performance of WLAN connection of UE according to UE location and SSID. The consumer can request either one-time or continuous reporting.

The service consumer may be an NF (e.g. PCF).

If a service consumer is PCF, the WLAN performance analytics can be used to update WLANSP as defined in TS 23.503 [4].

The consumer of these analytics may indicate in the request or subscription:

- Analytics ID = "WLAN performance";
- Target of Analytics Reporting: a single UE (SUPI), a group of UEs (an Internal Group ID), or any UE;
- Analytics Filter Information:
  - Area of Interest (list of TA or Cells);
  - SSID(s);
  - BSSID(s); and
  - optional list of analytics subsets that are requested (see clause 6.11.3);
- An Analytics target period indicates the time period over which the statistics or prediction are requested, either in the past or in the future;
- Optional maximum number of objects;
- Preferred level of accuracy of the analytics;
- Preferred level of accuracy per analytics subset (see clause 6.11.3);
- Preferred order of results for the list of WLAN performance information:

- ordering criterion: "time slot start", "number of UEs", "RSSI", "RTT" or "Traffic information"; and
- order: ascending or descending; and

- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

If the Target of Analytics Reporting is any UE, then the Analytics Filter should at least include Area of Interest or SSID(s) or BSSID(s).

6.11.2 Input Data

For the purpose of generating WLAN performance analytics results, the NWDAF collects the data as listed in Table 6.11.2-1.

Table 6.11.2-1: Data collected by NWDAF for WLAN performance analytics

Information	Source	Description
WLAN measurement results	OAM	The WLAN measurement results per wireless network served by the WLAN AP.
>SSID / BSSID / HESSID		SSID / BSSID / HESSID of the selected WLAN during the period of analysis.
> RSSI		Measured RSSI of the selected WLAN during the period of analysis.
> RTT		Measured RTT of the selected WLAN during the period of interest.
> UE Location		Location information tagged by UE when it reports WLAN MDT measurement (e.g. Cell ID and/or longitude/latitude if available).
Information on PDU Session for WLAN (1..max)	SMF	Information on PDU session for which Access Type is Non-3GPP and RAT Type is TRUSTED_WLAN.
>SSID / BSSID		SSID / BSSID that the PDU session is related to.
> Start time of the PDU Session for WLAN		The time stamp that indicates when the existing PDU Session's access type changes to WLAN or when the new PDU Session for WLAN is established.
> End time of the PDU Session for WLAN		The time stamp that indicates when the existing WLAN based PDU Session's access type is not WLAN any more or when the PDU Session for WLAN is released.
UE communications (1..max)	UPF	List of communication time slots
> Communication start		The time stamp that PDU session(s) for WLAN starts.
> Communication stop		The time stamp that PDU session(s) for WLAN ends.
> UL data rate		UL data rate of PDU session(s) for WLAN.
> DL data rate		DL data rate of PDU session(s) for WLAN.
> Traffic volume		Traffic volume of PDU session(s) for WLAN.

NOTE 1: WLAN Data from OAM is collected via MDT and aligned with the WLAN measurement reporting list described in clause 5.1.1.3.3 of TS 37.320 [20]. It is assumed that not all UEs support MDT WLAN measurements.

NOTE 2: How NWDAF collects UE communications related data from UPF is not defined in this Release of the specification.

NOTE 3: UE Location from OAM can be used to deduce WLAN location.

6.11.3 Output Analytics

The NWDAF generates WLAN performance analytics. Depending on the Analytics Target Period, the output consists of statistics or predictions. The detailed information provided by the NWDAF is defined in Table 6.11.3-1 for statistics and Table 6.11.3-2 for predictions.

Table 6.11.3-1: WLAN performance statistics

Information	Description
Area of Interest	A list of TAIs or Cell Ids
List of Analytics per SSID	SSIDs of WLAN access points deployed in the Area of Interest
> Time slot entry (1..max)	List of time slots during the Analytics target period
>> Time slot start	Time slot start time within the Analytics target period
>> Duration	Duration of the time slot
>> RSSI (NOTE 1)	Measured RSSI
>> RTT (NOTE 1)	Measured RTT
>> Traffic Information (NOTE 1)	UL/DL data rate, Traffic volume
>> Number of UEs (NOTE 1)	Number of UEs observed for the SSID
NOTE 1: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".	

Table 6.11.3-2: WLAN performance predictions

Information	Description
Area of Interest	A list of TAIs or Cell Ids
List of Analytics per SSID	SSIDs of WLAN access points deployed in the Area of Interest
> Time slot entry (1..max)	List of time slots during the Analytics target period
>> Time slot start	Time slot start time within the Analytics target period
>> Duration	Duration of the time slot
>> RSSI (NOTE 1)	Predicted RSSI
>> RTT (NOTE 1)	Predicted RTT
>> Traffic Information (NOTE 1)	Predicted UL/DL data rate, Traffic volume
>> Number of UEs (NOTE 1)	Number of UEs predicted for the SSID
>> Confidence	Confidence of the prediction
NOTE 1: This information element is an analytics subset that can be used in "list of analytics subsets that are requested" and "preferred level of accuracy per analytics subset".	

6.11.4 Procedures

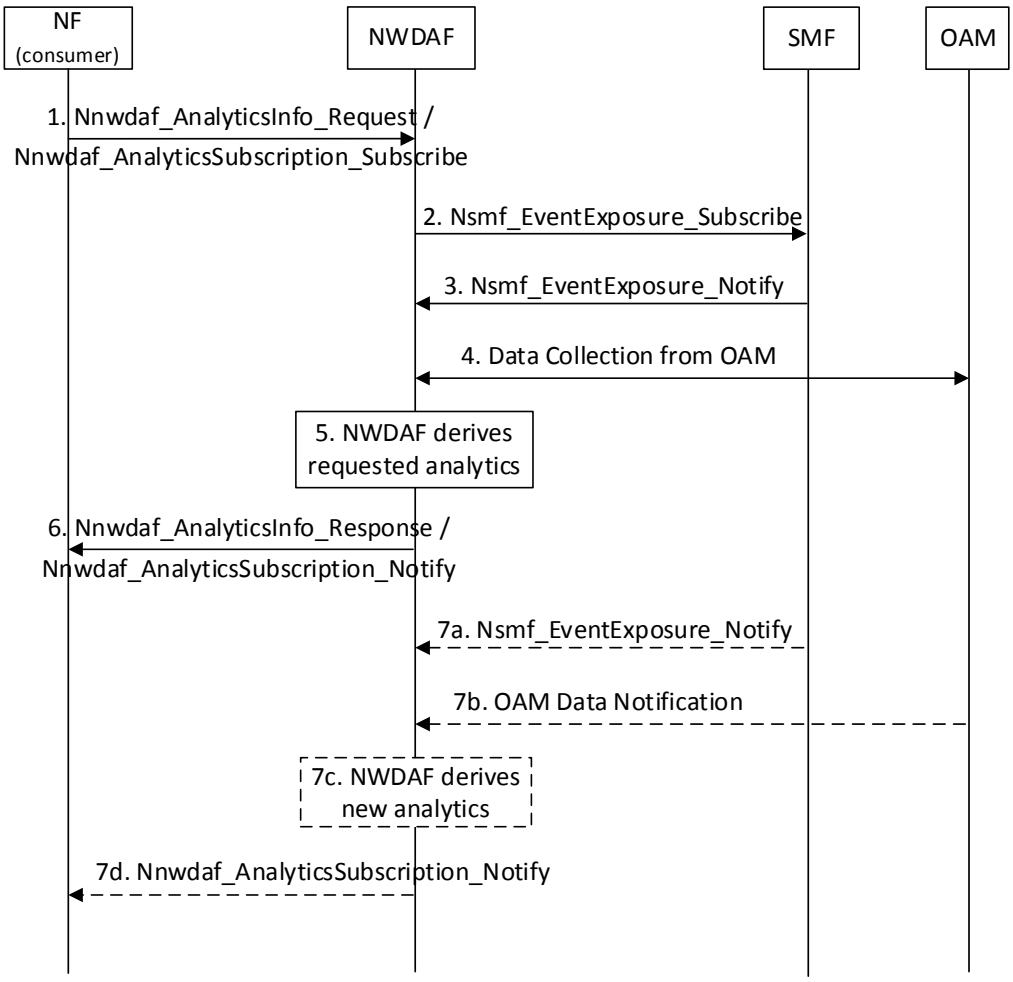

Figure 6.11.4-1: Procedure for WLAN performance analytics

1. The consumer NF sends a request to the NWDAF for WLAN performance analytics using either the Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription service. The Analytics ID is set to "WLAN performance", the Target of Analytics Reporting and the Analytics Filter Information are set according to clause 6.11.1. The consumer NF can request statistics or predictions.

   The analytics can be requested with the filter information (e.g. Area of Interest or specific SSID(s)). When Area of Interest is provided, the analytics results include WLAN performance information of all SSID(s) located in the Area of Interest. When specific SSID(s) is provided, the analytics results include WLAN performance information of a specific UE or all UE(s) connected to the corresponding SSID(s).

2-3. The NWDAF subscribes to information related to PDU Session for WLAN (i.e. Access Type is Non-3GPP and RAT Type is TRUSTED_WLAN) from SMF.

4. The NWDAF collects WLAN measurement data for the period of analysis from the OAM, following the procedure captured in clause 6.2.3.2.

NOTE: The NWDAF collects the data from the UPF as listed in Table 6.11.2.1. How the NWDAF collects the data is not defined in this Release of the specification.

5. The NWDAF derives requested analytics with the collected data. Analytics output parameters are listed in clause 6.11.3.

6. The NWDAF provides the requested analytics to the NF, using either the Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription service, depending on the service used at step 1.

7. If the NF subscribed the analytics at step 1, the NWDAF provides a new analytics when it generated the new output.

6.12 Session Management Congestion Control Experience Analytics

6.12.1 General

According to the Session Management Congestion Control (SMCC) mechanisms, i.e. DNN based congestion control defined in clause 5.19.7.3 of TS 23.501 [2] and S-NSSAI based congestion control defined in clause 5.19.7.4 of TS 23.501 [2], the SMF that is applying or has applied the SMCC mechanism does not store any historical information related to which UEs is/was subject to backoff timer settings. Therefore, fairness to apply the SMCC cannot be considered nor guaranteed. For example, among UEs that use a PDU Session associated with S-NSSAI#1, some of them may have experienced the S-NSSAI based high level of congestion control (e.g. receiving NAS SM reject messages with a long backoff timer) while some of the UEs may have experienced the S-NSSAI based low level congestion control (e.g. receiving NAS SM reject messages with a short backoff timer), within a specific period. The backoff timer provided to each UE can vary, e.g. up to 70 hours.

The SMF service consumer may request the NWDAF to provide Session Management Congestion Control Experience (SMCCE) statistical analytics for a specific DNN and/or S-NSSAI. The SMF uses potential congestion condition as a trigger to request the SMCCE analytics from the NWDAF.

The request by the SMF includes mainly the following parameters:

- Analytics ID = "Session Management Congestion Control Experience".
- Target of Analytics Reporting: one or more SUPI(s).

NOTE 1: The UE(s) contained in the Target of Analytics Reporting. These are UE(s) that have the PDU Session for the DNN and/or S-NSSAI indicated by Analytics Filter Information.

- Analytics Filter Information:
  - DNN and/or S-NSSAI; and
  - optional list of analytics subsets that are requested (see clause 6.12.3);
- Analytics target period: the time window for which the statistics are requested.

NOTE 2: Predictions are not provided as output for the Session Management Congestion Control Experience analytics.

6.12.2 Input Data

For the purpose of SMCCE analytics, the NWDAF collects the data as listed in Table 6.12.2-1.

Table 6.12.2-1: Data collected by NWDAF for SMCCE analytics

Information	Source	Description
UE ID	SMF	SUPI.
SMCC experience for PDU Session	SMF	Data related to SMCC experience per PDU Session.
> DNN	SMF	DNN for the PDU Session that SMF collects Data related to SMCCE.
> S-NSSAI	SMF	S-NSSAI for the PDU Session that SMF collects Data related to SMCCE.
> Start time of data collection	SMF	Start time of data collection.
> End time of data collection	SMF	End time of data collection.
>SM NAS request from UE (1..max)	SMF	Information on the SM NAS messages that SMF receives from UE for PDU Session during the collection period.
>> Type of SM NAS request	SMF	The type of SM NAS message transmitted by UE (e.g. PDU Session Establishment Request, PDU Session Modification Request, etc.).
>>Timestamp	SMF	A time stamp when SMF receives SM NAS message from UE.
> SM NAS message from network with backoff timer (1..max)	SMF	Information on SMCC applied to UE for PDU Session.
>> Type of SM NAS message from network	SMF	The type of SM NAS message with backoff timer provided to UE (e.g. PDU Session Establishment Reject, PDU Session Modification Reject, PDU Session Release Command, etc.).
>>Timestamp	SMF	A time stamp when SMF sends SM NAS message to UE.
>> Provided backoff timer	SMF	A value of backoff timer provided to UE.
>> Type of applied SMCC	SMF	The type of applied SMCC, i.e. DNN based congestion control or S-NSSAI based congestion control.

As described in Table 6.12.2-1, the NWDAF subscribes to the network data from SMF(s) by invoking Nsmf_EventExposure_Subscribe service (Event ID = Session Management Congestion Control Experience for PDU Session, Target of Event Reporting = one or more SUPI(s), Event Filter information = DNN and/or S-NSSAI and target period).

6.12.3 Output Analytics

The NWDAF outputs the SMCCE statistical analytics. The detailed statistical information provided by the NWDAF is defined in Table 6.12.3-1.

Table 6.12.3-1: SMCCE statistics

Information	Description
List of SMCCE Analytics (1..max)	
> DNN	DNN that SMCC is applied.
> S-NSSAI	S-NSSAI that SMCC is applied.
> List of UEs classified based on experience level of SMCC	One, or more than one, of the following lists (SUPI is used to identify a UE).
>> List of high-experienced UEs (NOTE 2)	A list of UEs whose experience level of SMCC for specific DNN and/or S-NSSAI is high.
>> List of medium-experienced UEs (NOTE 2)	A list of UEs whose experience level of SMCC for specific DNN and/or S-NSSAI is medium.
>> List of low-experienced UEs (NOTE 2)	A list of UEs whose experience level of SMCC for specific DNN and/or S-NSSAI is low.
NOTE 1: The high/medium/low-experience thresholds values are operator defined. NOTE 2: This information element is an analytics subset that can be used in "list of analytics subsets that are requested".	

6.12.4 Procedures

Figure 6.12.4-1 shows the procedure for Session Management Congestion Control Experience Analytics.

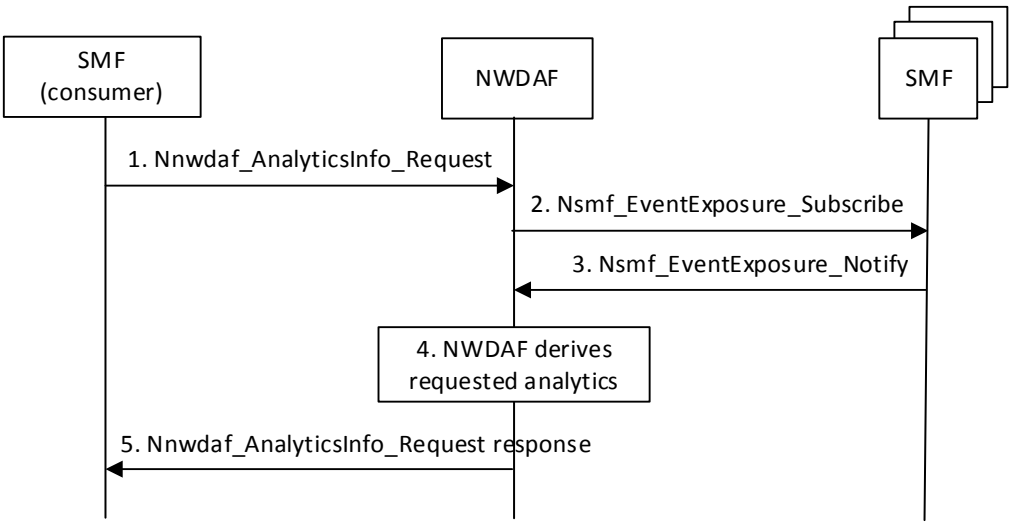

Figure 6.12.4-1: Procedure for Session Management Congestion Control Experience Analytics

1. Consumer SMF requests analytics information for "Session Management Congestion Control Experience" from the NWDAF when the SMF wants to take the analytics information into account for the Session Management Congestion Control to be applied.

   The parameters included in the request are described in clause 6.12.1.

NOTE: To account for SMCCE analytics information, the SMF needs to request the analytics information from the NWDAF before applying Session Management Congestion Control due to potential congestion conditions formation.

2. If has not already subscribed, the NWDAF sends subscription requests to all the SMFs serving the DNN and/or S-NSSAI as indicated by Analytics Filter Information to collect data related to SMCCE. The SMF that made the request in step 1 can be also one of the data providers.

3. The SMF(s) provide the collected data to the NWDAF.

4. The NWDAF derives the requested analytics.

5. The NWDAF provides the analytics for Session Management Congestion Control Experience to the consumer SMF.

6.13 Redundant Transmission Experience related analytics

6.13.1 General

This clausedescribes the Redundant Transmission Experience related analytics. This analytics may be used by the SMF to determine whether redundant transmission shall be performed, or (if it had been activated) shall be stopped.

The service consumer may be a NF (e.g. SMF).

The consumer of these analytics may indicate in the request:

- Analytics ID = "Redundant Transmission Experience".
- Target of Analytics Reporting: a single UE (SUPI), any UE, or a group of UEs (an Internal Group ID).
- Analytics Filter Information optionally containing:
  - Area of Interest;
  - S-NSSAI;
  - DNN.

- An Analytics target period indicates the time period over which the statistics or predictions are requested.
- Preferred level of accuracy of the analytics;
- Preferred order of results for the list of Redundant Transmission Experience:
  - ordering criterion: "time slot start" or "Redundant Transmission Experience"; and
  - order: ascending or descending;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

6.13.2 Input Data

The NWDAF supporting data analytics on Redundant Transmission Experience shall be able to collect UE mobility information from OAM, 5GC and AFs, and service data from AF, as described in clause 6.7.2.2. In addition, it shall be able to collect the information for PDU session which is established with redundant transmission from NF and OAM. UE mobility information is specified in Table 6.7.2.2-1 and service data from AF related to UE mobility in Table 6.7.2.2-2. In addition, it shall be able to collect performance measurement on user data congestion as specified in Table 6.8.2-1.

Additionally, the NWDAF collects the following input (see Table 6.13.2-1 and Table 6.13.2-2) according to existing measurements defined in clause 5.33.3 QoS Monitoring to Assist URLLC Service of TS 23.501 [2].

Table 6.13.2-1: Packet drop and/or packet delay measurement per QFI or GTP level

Information	Source	Description
UL/DL packet drop GTP	OAM (see NOTE 3)	UL/DL packet drop rate measurement on GTP path on N3.
UL/DL packet delay GTP	UPF (see NOTE 2)	End-to-End measurements from UE to UPF.
UL/DL packet delay GTP	OAM (see NOTE 3)	UL/DL packet delay measurement round trip on GTP path on N3.
NOTE 1: The information in this table is provided both as the base to compare with the redundant transmission performance as well as when redundant transmission is enabled. NOTE 2: How NWDAF collects the information from UPF is not defined in this specification. NOTE 3: Refer to clause 5.1 of TS 28.552 [8] for the performance measurement in NG-RAN and clause 5.4 1 of TS 28.552 [8] for the performance measurement in UPF. In addition, Annex A of TS 28.552 [8] describes various performance measurements, in particular, clause A.61 indicates that the measurements on the one way DL and UL delay between PSA UPF and NG-RAN can be used to evaluate and optimize the DL and UL user plane delay performance between 5GC and NG-RAN. NOTE 4: The NWDAF data collection request/subscription will not activate the measurements for QoS Monitoring. When QoS Monitoring is activated the measurements are triggered according to existing procedures. When QoS Monitoring is not activated SMF may per configuration activate measurements for QoS Monitoring at least at the same time as it requests Analytics.		

Table 6.13.2-2: The information related to PDU Session established with redundant transmission

Information	Source	Description
DNN	SMF	Data Network Name associated for URLLC service.
UP with redundant transmission	SMF	Redundant transmission setup.

6.13.3 Output Analytics

The NWDAF supporting data analytics on Redundant Transmission Experience shall be able to provide Redundant Transmission Experience analytics as defined in Table 6.13.3-1 and Table 6.13.3-2.

Table 6.13.3-1: Redundant Transmission Experience statistics

Information	Description
UE group ID or UE ID, any UE	Identifies a UE, any UE, or a group of UEs.
DNN	Data Network Name associated for URLLC service.
Spatial validity	Area where the Redundant Transmission Experience applies. If Area of Interest information was provided in the request or subscription, spatial validity should be the requested Area of Interest..
Time slot entry (1..max)	List of time slots during the Analytics target period.
> Time slot start	Time slot start within the Analytics target period.
> Duration	Duration of the time slot (average and variance).
> Redundant Transmission Experience	Redundant Transmission Experience value.
> Ratio	Percentage on which UE, any UE, or UE group efficiently use the PDU session with redundant transmission.

Table 6.13.3-2: Redundant Transmission Experience predictions

Information	Description
UE group ID or UE ID, any UE	Identifies a UE or, any UE, a group of UEs.
DNN	Data Network Name associated for URLLC service.
Spatial validity	Area where the estimated Redundant Transmission Experience applies. If Area of Interest information was provided in the request or subscription, spatial validity should be the requested Area of Interest.
Time slot entry (1..max)	List of predicted time slots.
>Time slot start	Time slot start time within the Analytics target period.
> Duration	Duration of the time slot.
> Redundant Transmission Experience	Predicted Redundant Transmission Experience value during the Analytics target period.
> Ratio	Percentage on which the UE, any UE, or UE group may efficiently use the PDU session with redundant transmission.
> Confidence	Confidence of this prediction.

6.13.4 Procedures

6.13.4.1 Analytics Procedure

Figure 6.13.4.1-1 shows the analytics procedure. The NWDAF can provide analytics, in the form of statistics or predictions or both.

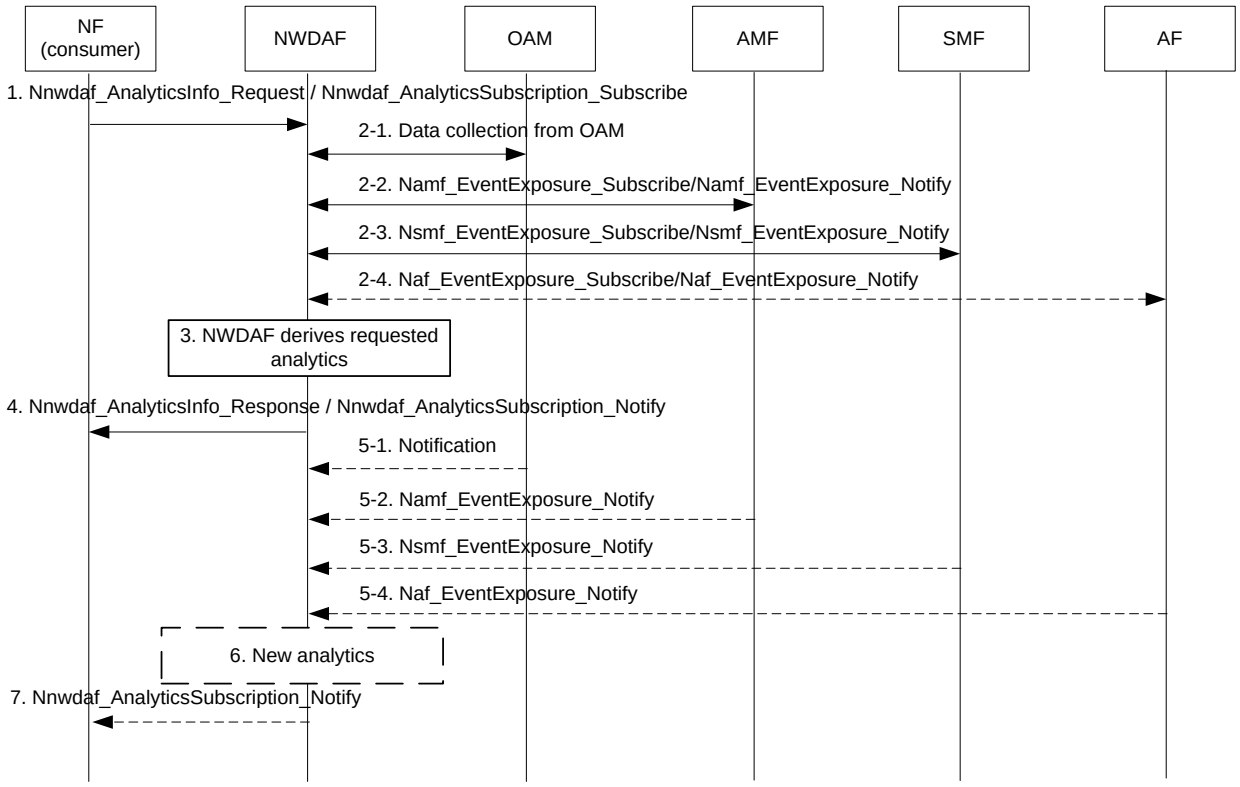

Figure 6.13.4.1-1: Redundant Transmission Experience analytics provided to an NF

1. The analytics consumer sends a request to the NWDAF for analytics on a specific UE, any UE, or a group of UEs, using either the Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription service. The NF can request statistics or predictions or both. The type of analytics is set to Redundant Transmission Experience. The NF provides the UE id or Internal Group ID in the Target of Analytics Reporting. Analytics Filter Information optionally contains DNN, S-NSSAI, Area of Interest, etc.

2. If the request is authorized, and in order to provide the requested analytics, the NWDAF may subscribe to events with all the serving AMFs for notification of location changes, and may subscribe to events with SMFs serving PDU Session on URLLC service for notification of redundant transmission related information.

   The NWDAF may subscribe the service data from AF(s) by invoking Naf_EventExposure_Subscribe service or Nnef_EventExposure_Subscribe (if via NEF).

   The NWDAF collects UE mobility information, packet measurement information and/or redundant transmission related information from OAM, following the procedure captured in clause 6.2.3.2.

NOTE: The NWDAF determines the AMF serving the UE, any UE, or the group of UEs as described in clause 6.2.2.1.

   This step may be skipped when e.g. the NWDAF already has the requested analytics available.

3. The NWDAF derives requested analytics.

4. The NWDAF provide requested UE Presence Pattern analytics to the NF, using either the Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1.

5-7. If at step 1, the NF has subscribed to receive notifications for Redundant Transmission Experience analytics, after receiving event notification from the AMFs, AFs and OAM subscribed by NWDAF in step 2, the NWDAF may generate new analytics and provide them to the NF.

If a service consumer is SMF, the Redundant Transmission Experience analytics can be used to make decision if that redundant transmission shall be performed or (if activated) shall be stopped regarding the PDU session for URLLC service.

6.14 DN Performance Analytics

6.14.1 General

This clause specifies how an NWDAF can provide DN Performance Analytics which provides analytics for user plane performance (i.e. average/maximum traffic rate, average/maximum packet delay, average packet loss rate) in the form of statistics or predictions to a service consumer.

The DN Performance Analytics may provide one or a combination of the following information:

- User plane performance analytics for a specific Edge Computing application for a UE, group of UEs, or any UE over a specific serving anchor UPF.
- User plane performance analytics for a specific Edge Computing application for a UE, group of UEs, or any UE over a specific DNAI.
- User plane performance analytics for a specific Edge Computing application for a UE, group of UEs, or any UE over a specific Edge Application Server Instance.

The service consumer may be an NF (e.g. SMF) or an AF.

The consumer of these analytics shall indicate in the request or subscription:

- Analytics ID = "DN Performance";
- Target of Analytics Reporting: one or more SUPI(s) or Internal Group Identifier(s), or "any UE";
- Analytics Filter Information as defined in table 6.14.1-1; and
- optionally, a preferred level of accuracy of the analytics;
- optionally, preferred level of accuracy per analytics subset (see clause 6.14.3);
- optionally, preferred order of results for the list of Network Performance information:
  - ordering criterion: one of the analytics subset (see clause 6.14.3);
  - order: ascending or descending;
- optionally, Reporting Thresholds, which apply only for subscriptions and indicate conditions on the level to be reached for respective analytics subsets (see clause 6.14.3) in order to be notified by the NWDAF;
- optionally, maximum number of objects and maximum number of SUPIs.

Table 6.14.1-1: Analytics Filter Information related to DN Performance Analytics

Information	Description
Application ID (0..max)	The identification of the application(s) for which the analytics information is subscribed or requested.
S-NSSAI	Identifies the Network Slice for which analytics information is subscribed or requested.
NSI ID(s)	Identifies the Network Slice instance(s) for which analytics information is subscribed or requested.
Area of Interest	Identifies the Area (i.e. set of TAIs), as defined in TS 23.501 [2] for which the analytics information is subscribed or requested.
UPF anchor identity	Identifies the UPF where a UE has an associated PDU session.
DNN	DNN to access the application.
DNAI	Identifier of a user plane access to one or more DN(s) where applications are deployed as defined in TS 23.501 [2].
Application Server Address(es)	List of IP address(s)/FQDN(s) of the Application Server(s) that a UE, group of UEs, or 'any UE' has a communication session with for which DN Performance Analytic information is requested.
List of analytics subsets	List of analytics subsets that are requested among those specified in clause 6.14.3.
NOTE: All parameters are optional.	

6.14.2 Input Data

The data collected from the AF are defined in table 6.14.2-1

Table 6.14.2-1: Performance Data from AF

Information	Source	Description
UE identifier	AF	IP address of the UE at the time the measurements was made.
UE location	AF	The location of the UE when the performance measurement was made.
Application ID	AF	To identify the service and support analytics per type of service (the desired level of service).
IP filter information	AF	Identify a service flow of the UE for the application.
Locations of Application	AF/NEF	Locations of application represented by a list of DNAI(s). The NEF may map the AF-Service-Identifier information to a list of DNAI(s) when the DNAI(s) being used by the application are statically defined.
Application Server Instance address	AF/NEF	The IP address/FQDN of the Application Server that the UE had a communication session when the measurement was made.
Performance Data	AF	The performance associated with the communication session of the UE with an Application Server that includes: Average Packet Delay, Average Loss Rate and Throughput.
Timestamp	AF	A time stamp associated to the Performance Data provided by the AF.

The data collected by the SMF are described in table 6.4.2-2.

The NWDAF subscribes to network data as defined in clause 6.4.2.

Data may be collected from OAM as described in table 6.4.2-3 by using the services provided by OAM as described in clause 6.2.3.

The Event Filters for the service data collection from SMF, AMF and AF are defined in TS 23.502 [3].

The timestamps are provided by each NF to allow correlation of QoS and traffic KPIs. The clock reference is able to know the accuracy of the time and correlate the time series of the data retrieved from each NF.

6.14.3 Output Analytics

The DN performance analytics is shown in table 6.14.3-1 and table 6.14.3-2.

Table 6.14.3-1: DN service performance statistics

Information	Description
Application ID	Identifies the application for which analytics information is provided.
S-NSSAI	Identifies the Network Slice for which analytics information is provided. See note 1.
DNN	Identifies the data network name (e.g. "internet") for which analytics information is provided. See NOTE 1.
DN performance (0-x)	List of DN performances for the application.
> Application Server Instance Address	Identifies the Application Server Instance (IP address/FQDN of the Application Server).
>Serving anchor UPF	The involved anchor UPF. See NOTE 2.
> DNAI	Identifier of a user plane access to one or more DN(s) where applications are deployed as defined in TS 23.501 [2].
>Performance	Performance indicators.
>> Average Traffic rate	Average traffic rate observed for UEs communicating with the application. See NOTE 3.
>> Maximum Traffic rate	Maximum traffic rate observed for UEs communicating with the application. See NOTE 3.
>>Average Packet Delay	Average packet delay observed for UEs communicating with the application. See NOTE 3.
>>Maximum Packet Delay	Maximum packet delay for observed for UEs communicating with the application. See NOTE 3.
>> Average Packet Loss Rate	Average packet loss observed for UEs communicating with the application. See NOTE 3.
>Spatial Validity Condition	Area where the DN performance analytics applies.
>Temporal Validity Condition	Validity period for the DN performance analytics.
NOTE 1: The item "DNN" and "S-NSSAI" shall not be included if the consumer NF is an untrusted AF. NOTE 2: The item "Serving anchor UPF" shall not be included if the consumer is an AF. NOTE 3: Analytics subset that can be used in "list of analytics subsets that are requested", "Preferred level of accuracy per analytics subset" and "Reporting Thresholds".	

Table 6.14.3-2: DN service performance predictions

Information	Description
Application ID	Identifies the application for which analytics information is provided.
S-NSSAI	Identifies the Network Slice for which analytics information is provided. See NOTE 1.
DNN	Identifies the data network name (e.g. internet) for which analytics information is provided. See NOTE 1.
DN performance (0-x)	List of DN performance for the application.
> Application Server Instance Address	Identifies the Application Server Instance (IP address/FQDN of the Application Server).
>Serving anchor UPF	The involved anchor UPF. See NOTE 2.
> DNAI	Identifier of a user plane access to one or more DN(s) where applications are deployed as defined in TS 23.501 [2].
>Performance	Performance indicators
>> Average Traffic rate	Average traffic rate predicted for UEs communicating with the application. See NOTE 3.
>> Maximum Traffic rate	Maximum traffic rate predicted for UEs communicating with the application. See NOTE 3.
>>Average Packet Delay	Average packet delay predicted for UEs communicating with the application. See NOTE 3.
>>Maximum Packet Delay	Maximum packet delay for predicted for UEs communicating with the application. See NOTE 3.
>> Average Packet Loss Rate	Average packet loss predicted for UEs communicating with the application. See NOTE 3.
>Spatial Validity Condition	Area where the DN performance analytics applies.
>Temporal Validity Condition	Validity period for the DN performance analytics.
>Confidence	Confidence of this prediction.
NOTE 1: The item "DNN" and "S-NSSAI" shall not be included if the consumer is an untrusted AF. NOTE 2: The item "Serving anchor UPF" shall not be included if the consumer is an AF. NOTE 3: Analytics subset that can be used in "list of analytics subsets that are requested", "Preferred level of accuracy per analytics subset" and "Reporting Thresholds".	

6.14.4 Procedures to request DN Performance Analytics for an Application

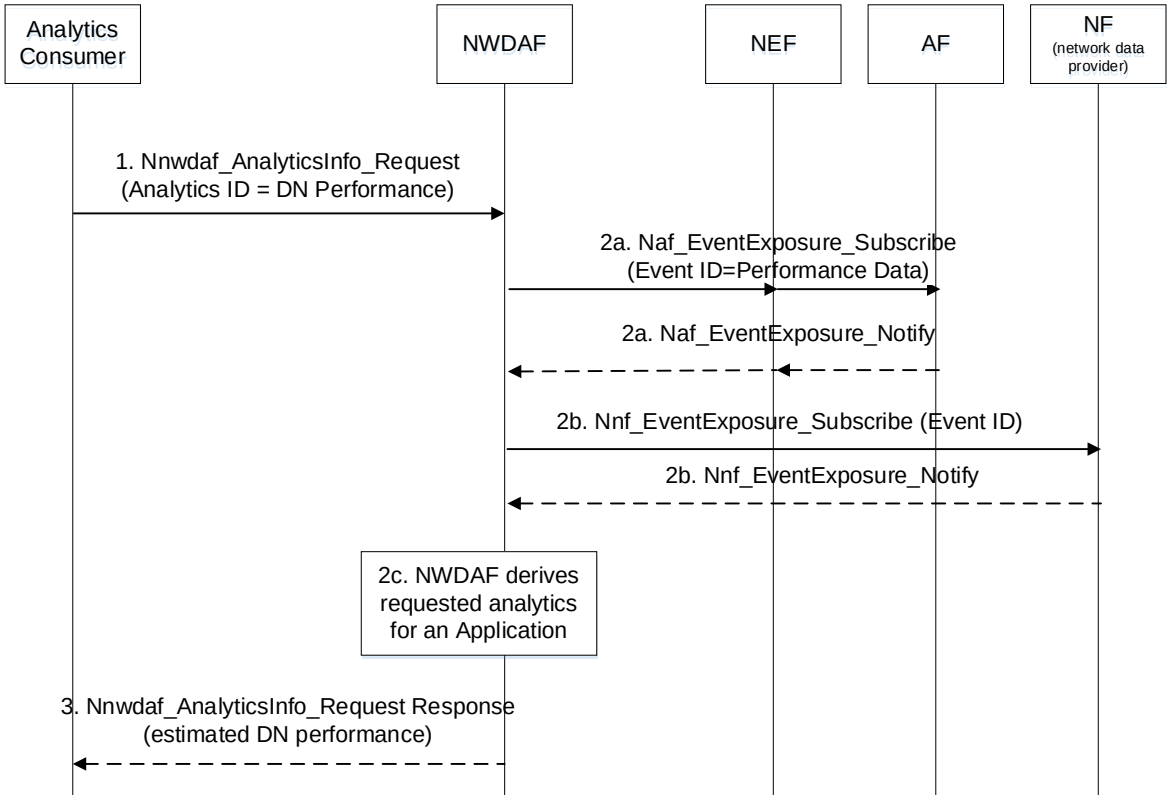

Figure 6.14.4-1: Procedure for NWDAF providing DN Performance analytics for an Application

The procedure illustrated in figure 6.14.4-1 allows an analytics consumer to request Analytics ID "DN Performance" for a particular Application. The analytics consumer includes the Application ID for which DN Performance is requested. The consumer indicates the Target of Analytics Reporting (e.g. "any UE") and may include as Analytic Filter Information the UPF anchor ID, DNAI, or Application Server instance that DN performance analytics are requested.

1. Analytics consumer sends an Analytics request/subscribe (Analytics ID = DN Performance Target of Analytics Reporting, Analytics Filter Information = (Application ID, S-NSSAI, DNN, Area of Interest, UPF anchor ID, DNAI, Application Server Address(es)), Analytics Reporting Information=Analytics target period) to NWDAF by invoking a Nnwdaf_AnalyticsInfo_Request or a Nnwdaf_AnalyticsSubscription_Subscribe service.

2a. NWDAF subscribes to the performance data from AF defined in table 6.14.2-1 by invoking Nnef_EventExposure_Subscribe or Naf_EventExposure_Subscribe service (Event ID = Performance Data, Application ID, Event Filter information), Target of Event Reporting = Any UE) as defined in TS 23.502 [3].

NOTE 1: In the case of trusted AF, NWDAF provides the Area of Interest as a list of TAIs to AF. In the case of untrusted AF, NEF translates the requested Area of Interest provided as event filter by NWDAF into geographic zone identifier(s) that act as event filter for AF.

2b. NWDAF subscribes to the network data from 5GC NF(s) defined in table 6.4.2-2 by invoking Nnf_EventExposure_Subscribe service.

2c. With the collected data, the NWDAF estimates the DN Performance for the application.

3. NWDAF provides the data analytics, to the analytics consumer by means of either Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1.

NOTE 2: For simplicity, the call flow only shows a request-response model for the interaction of NWDAF and analytics consumer instead of both request-response model and subscription-notification model.

If the analytics consumer is an SMF, the SMF may use the analytics to determine the UPF and DNAI that offers the best user plane performance.

If the analytics consumer is an AF, the AF may use the analytics to determine the DNAI that has the best user plane performance if Application Server relocation is required.

6.15 Void

7 Nnwdaf Services Description

7.1 General

Table 7.1-1 illustrates the NWDAF Services.

Table 7.1-1: NF services provided by NWDAF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnwdaf_AnalyticsSubscription	Subscribe	Subscribe / Notify	PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF, NWDAF, DCCF
	Unsubscribe		PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF, NWDAF, DCCF
	Notify		PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF, NWDAF, DCCF, MFAF
	Transfer	Request / Response	NWDAF
Nnwdaf_AnalyticsInfo	Request	Request / Response	PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF, NWDAF, DCCF
	Transfer	Request / Response	NWDAF
Nnwdaf_DataManagement	Subscribe	Subscribe / Notify	NWDAF, DCCF
	Notify		NWDAF, DCCF, MFAF
	Fetch	Request / Response	NWDAF, DCCF, MFAF
Nnwdaf_MLModelProvision	Subscribe	Subscribe / Notify	NWDAF
	Unsubscribe		NWDAF
	Notify		NWDAF
Nnwdaf_MLModelInfo	Request	Request / Response	NWDAF
NOTE 1: How OAM consumes Nnwdaf services and which Analytics information is relevant is defined in TS 28.550 [7] Annex H and out of the scope of this TS. NOTE 2: How CEF consumes Nnwdaf services and which Analytics information is relevant is defined in TS 28.201 [21] and out of the scope of this TS. NOTE 3: The Nnwdaf_MLModelProvision service and the Nnwdaf_MLModelInfo service are provided by an NWDAF containing MTLF and consumed by an NWDAF containing AnLF.			

Table 7.1-2 shows the analytics information provided by NWDAF service.

Table 7.1-2: Analytics information provided by NWDAF

Analytics Information	Request Description	Response Description
Slice Load level information	Analytics ID: load level information	Load level provided as number of UE registrations and number of PDU sessions for a Network Slice and Network Slice instances as well as resource utilization for Network Slice instances.
Observed Service experience information	Analytics ID: Service Experience	Observed Service experience statistics or predictions may be provided for a Network Slice or an Application. They may be derived from an individual UE, a group of UEs or any UE. For slice service experience, they may be derived from an Application, a set of Applications or all Applications on the Network Slice.
NF Load information	Analytics ID: NF load information	Load statistics or predictions information for specific NF(s).
Network Performance information	Analytics ID: Network Performance	Statistics or predictions on the load in an Area of Interest; in addition, statistics or predictions on the number of UEs that are located in that Area of Interest.
UE mobility information	Analytics ID: UE Mobility	Statistics or predictions on UE mobility. When visited AOI(s) is included in the Analytics Filter information, only statistics on UE mobility can be provided.
UE Communication information	Analytics ID: UE Communication	Statistics or predictions on UE communication.
Expected UE behavioural parameters	Analytics ID: UE Mobility and/or UE Communication	Analytics on UE Mobility and/or UE Communication.
UE Abnormal behaviour information	Analytics ID: Abnormal behaviour	List of observed or expected exceptions, with Exception ID, Exception Level and other information, depending on the observed or expected exceptions.
User Data Congestion information	Analytics ID: User Data Congestion	Statistics or predictions on the user data congestion for transfer over the user plane, for transfer over the control plane, or for both.
QoS Sustainability	Analytics ID: QoS Sustainability	For statistics, the information on the location and the time for the QoS change and the threshold(s) that were crossed; or, for predictions, the information on the location and the time when a potential QoS change may occur and what threshold(s) may be crossed.
Session Management Congestion Control Experience	Analytics ID: Session Management Congestion Control Experience	Statistics on session management congestion control experience for specific DNN and/or S-NSSAI.
Redundant Transmission Experience	Analytics ID: Redundant Transmission Experience	Statistics or predictions aimed at supporting redundant transmission decisions for URLLC services.
WLAN performance	Analytics ID: WLAN performance	Statistics or predictions on WLAN performance of UE.
Dispersion	Analytics ID: UE Dispersion	Statistics or predictions that identify the location (i.e. areas of interest) or network slice(s) where a UE, or a group of UEs disperse their data volume, or disperse mobility or session management transactions or both.
DN Performance	Analytics ID: DN Performance	Statistics or predictions on user plane performance for a specific Edge Computing application.

7.2 Nnwdaf_AnalyticsSubscription Service

7.2.1 General

Service Description: This service enables the consumer to subscribe/unsubscribe for network data analytics.

When the subscription for network data analytics is accepted by the analytics NWDAF, the consumer receives from the NWDAF an identifier (Subscription Correlation ID) allowing to further manage (modify, delete) this subscription. The modification of Analytics subscription can be enforced by NWDAF based on operator policy and configuration.

This service also enables the consumer to transfer analytics subscriptions to another NWDAF using the Nnwdaf_AnalyticsSubscription_Transfer service operation. Using this service operation, a consumer can request to the NWDAF to prepare for or take over analytics subscription(s), indicating also if and where analytics context is available.

7.2.2 Nnwdaf_AnalyticsSubscription_Subscribe service operation

Service operation name: Nnwdaf_AnalyticsSubscription_Subscribe.

Description: Subscribes to NWDAF analytics with specific parameters.

Inputs, Required:

- (Set of) Analytics ID(s) as defined in Table 7.1-2;
- Target of Analytics Reporting;
- Notification Target Address (+ Notification Correlation ID);
- Analytics Reporting Parameters (including Analytics target period, etc.).

NOTE 1: Target of Analytics Reporting can be provided per individual Analytics ID.

Inputs, Optional:

- Analytics Filter Information;
- Subscription Correlation ID (in the case of modification of the analytics subscription);
- preferred level of accuracy of the analytics;
- preferred level of accuracy per analytics subset;
- Reporting Thresholds;
- maximum number of objects requested (max);
- preferred order of results,maximum number of SUPIs requested (SUPImax);
- time when analytics information is needed;
- Analytics Metadata Request;
- (Set of) NWDAF identifiers used by the NWDAF service consumer when aggregating multiple analytic subscriptions;
- Dataset Statistical Properties;
- Output strategy;
- Data time window;
- consumer NF's serving area or NF ID;

- information of previous analytics subscription, i.e. NWDAF identifier (i.e. Instance ID or Set ID), Analytics ID(s), and Subscription Correlation ID and optionally associated Analytics specific data (according to clause 5.2.2.2.2 of TS 23.502 [3]).

NOTE 2: Analytics Filter Information, Reporting Thresholds, maximum number of objects requested (max),maximum number of SUPIs requested (SUPImax), Analytics Metadata Request, Dataset Statistical Properties, Output strategy, Data time window and time when analytics information is needed can be provided per individual Analytics ID.

Outputs Required: When the subscription is accepted: Subscription Correlation ID (required for management of this subscription). When the subscription is not accepted, an error response.

Outputs, Optional: None.

NOTE 3: When the Target of Analytics Reporting is a SUPI or a GPSI then the subscription may not be accepted, e.g. user consent is not granted, and an error is sent to the consumer. When the Target of Analytics Reporting is an Internal Group Id, or a list of SUPIs/GPSI(s) or any UE, no error is sent, but a SUPI or GPSI is skipped if user consent is not granted.

7.2.3 Nnwdaf_AnalyticsSubscription_Unsubscribe service operation

Service operation name: Nnwdaf_AnalyticsSubscription_Unsubscribe.

Description: Unsubscribe to NWDAF analytics.

Inputs, Required: Subscription Correlation ID.

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

7.2.4 Nnwdaf_AnalyticsSubscription_Notify service operation

Service operation name: Nnwdaf_AnalyticsSubscription_Notify.

Description:NWDAF notifies the consumer instance of the analytics that has subscribed to the specific NWDAF service. See also clause 6.1.3 for contents of the Analytics Exposure.

Inputs, Required: Notification Correlation Information: this parameter indicates the Notification Correlation Id that has been assigned by the consumer during analytics subscription.

Inputs, Optional:

- Set of the tuple (Analytics ID, Analytics specific parameters): this parameter shall be present if output analytics are reported.
- Timestamp of analytics generation.
- Validity period.
- Confidence
- Revised waiting time.
- Analytics Metadata Information.
- Termination Request: this parameter indicates that NWDAF requests to terminate the analytics subscription, i.e., NWDAF will not provide further notifications related to this subscription, with cause value (e.g. user consent revoked, NWDAF overload, UE moved out of NWDAF serving area, etc.).

NOTE: Validity period can also be provided as part of Analytics specific parameters for some NWDAF output analytics.

- Subscription Change Notification Correlation ID: this parameter shall be present if the notification is for informing the assignment of a new Subscription Correlation Id by the NWDAF. It is set to the old Subscription Correlation ID.
- Subscription Correlation ID: this parameter shall be present if the notification is for informing the assignment of a new Subscription Correlation Id by the NWDAF. It is set to a new Subscription Correlation ID assigned by the NWDAF.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

7.2.5 Nnwdaf_AnalyticsSubscription_Transfer service operation

Service operation name: Nnwdaf_AnalyticsSubscription_Transfer.

Description: Requests to NWDAF to transfer analytics subscription(s) from the consumer NWDAF.

Inputs, Required:

- Transfer type: indicates the type of the transfer request. The following values are supported:
  - Analytics subscription transfer preparation: requests the NWDAF to prepare for taking over the analytics subscription(s) and/or prepare for collecting Analytics Context(s).
  - Analytics subscription transfer: requests the NWDAF to take over the analytics subscription(s).
  - Analytics subscription transfer cancel: cancels a prepared analytics subscription request.

Inputs, Optional:

- If this service operation is for "analytics subscription transfer preparation", the following parameter shall be provided:
  - (Set of) analytics subscription information with the following parameters:
    - All input parameters for the analytics exposure as specified in clause 6.1.3.
    - [OPTIONAL] Active data source ID(s): Instance ID or Set ID of the active data source(s) the consumer NWDAF is currently using for the analytics of this analytics subscription.
    - [OPTIONAL] Model information related to the ML model(s) that the NWDAF is currently using for the analytics:
      - File address of the ML model(s).
      - [OPTIONAL] ID(s) of NWDAF(s) containing MTLF: Instance ID(s) of the NWDAF(s) containing MTLF from which the consumer NWDAF currently subscribes to the ML model information used for the analytics.
    - ID of the analytics consumer, e.g. NF, AF or OAM, that is subscribed to receive analytics.
    - (Set of) analytics context identifier(s): identifies analytics context available at the consumer NWDAF as defined in clause 6.1B.4.
- If this service operation is to request analytics subscriptions transfer and if analytics subscription transfer preparation is not performed, the same parameters as those for transfer type "Analytics subscription transfer preparation" shall be provided.
- If this service operation is to request analytics subscriptions transfer and if analytics subscription transfer preparation is performed, the same parameters as those for transfer type "Analytics subscription transfer preparation" can be provided with updated parameter values.
- If this service operation is to request analytics subscriptions transfer cancel, the following parameter shall be provided:

- Subscription Correlation ID.

Outputs Required: Operation execution result indication.

Outputs, Optional: None.

7.3 Nnwdaf_AnalyticsInfo service

7.3.1 General

Service description: this service enables the consumer to request and get from NWDAF network data analytics or enables NWDAF to request transfer of analytics context from another NWDAF.

7.3.2 Nnwdaf_AnalyticsInfo_Request service operation

Service operation name: Nnwdaf_AnalyticsInfo_Request.

Description: The consumer requests NWDAF operator specific analytics.

Inputs, Required: (Set of) Analytics ID(s) as defined in Table 7.1-2, Target of Analytics Reporting, Analytics Reporting Parameters (including Analytics target period, etc..

NOTE 1: Target of Analytics Reporting can be provided per individual Analytics ID.

Inputs, Optional: Analytics Filter Information, preferred level of accuracy of the analytics,preferred level of accuracy per analytics subset, time when analytics information is needed, maximum number of objects requested (max),preferred order of results,maximum number of SUPIs requested (SUPImax), Analytics Metadata Request, Dataset Statistical Properties, Output strategy and Data time window.

NOTE 2: Analytics Filter Information, Maximum number of objects requested (max), Maximum number of SUPIs requested (SUPImax), Analytics Metadata Request, Dataset Statistical Properties, Output strategy, Data time window and time when analytics information is needed can be provided per individual Analytics ID.

Outputs, Required: If the request is accepted, then set of the tuple (Analytics ID, Analytics specific parameters). When the request is not accepted, an error response.

Outputs, Optional: Timestamp of analytics generation, validity period, confidence, revised waiting time, Analytics Metadata Information. See clause 6.1.3.

NOTE 3: Validity period can also be provided as part of Analytics specific parameters for some NWDAF output analytics.

NOTE 4: When the Target of Analytics Reporting is a SUPI or a GPSI then the request may not be accepted, e.g. user consent is not granted, and an error is sent to the consumer. When the Target of Analytics Reporting is an Internal Group Id, or a list of SUPIs/GPSI(s) or any UE, no error is sent, but a SUPI or GPSI is skipped if user consent is not granted.

7.3.3 Nnwdaf_AnalyticsInfo_ContextTransfer service operation

Service operation name: Nnwdaf_AnalyticsInfo_ContextTransfer.

Description: Requests to NWDAF to transfer context information related to analytics subscriptions.

Inputs, Required: (Set of) Analytics context identifier(s).

Inputs, Optional: Requested Analytics Context per analytics context identifier.

Outputs Required: (Set of) Analytics Context as specified in clause 6.1B.4.

Outputs, Optional: ADRF ID with Analytics Context Type stored in the ADRF (i.e., Historical output Analytics and/or Data related to Analytics).

NOTE: For the Requested Analytics Context, the NWDAF can return a combination of Analytics Context and reference to ADRF ID from where Historical output Analytics and/or Data related to Analytics can be retrieved.

7.4 Nnwdaf_DataManagement Service

7.4.1 General

Service Description: This service enables the consumer to subscribe/unsubscribe, be notified about data exposed by NWDAF, or fetch the subscribed data. It enables the consumer to request the generation of bulked data for Event IDs from NFs, as well as for Analytics IDs and retrieve the requested data.

7.4.2 Nnwdaf_DataManagement_Subscribe service operation

Service operation name: Nnwdaf_DataManagement_Subscribe.

Description: The consumer subscribes to receive data or historical analytics which is regarded as a kind of data, or if the data is already defined in NWDAF, then the subscription is updated.

Inputs, Required: Data Specification or Analytics Specification, Notification Target Address (+ Notification Correlation ID).

When the required data is a bulked data for Event IDs received from NFs, the Data Specification includes: set of Event IDs, Event Filter Information, Target of Event Reporting, and bulked data type as defined in clause 6.2.6.1.

When the required data is a bulked data for Analytics ID, the Data Specification includes: Target of Reporting with the set of Analytics ID(s) to generate bulked data, bulked data type, and analytics stage; Filter Information with Target of Analytics Information, Analytics Filter Information as defined in clause 6.2.6.1.

When the required data is historical analytics, the Analytics Specification is included in the required input parameters and identifies the historical analytics to be collected, the Analytics Specification includes: Analytics ID(s), Target of Analytics Reporting, Analytics Filter information and other input parameters for NWDAF services as defined in clause 7.2 and clause 7.3.

NOTE 1: Event Filter Information, Target of Event Reporting and Bulked data type can be provided per individual Event ID in a set of Event IDs to generate bulked data.

NOTE 2: Bulked data type, analytics stage, Target of Analytics Information, Analytics Filter Information can be provided per individual Analytics ID in a set of Analytics IDs to generate bulked data.

Inputs, Optional: Service Operation, Bulked Data Formatting and Processing, Data Source, ADRF information to store data used for generated bulked data, ADRF ID or NWDAF ID (or ADRF Set ID or NWDAF Set ID) storing historical data to be used for bulked data generation.

The Bulked Data Formatting and Processing parameters include: the parameters defined in clause 5A.4 as well as Periodic bulked data notification, Feature type, Time Window, Minimum and/or maximum number of samples, Fetch flag, Bulked data deadline, Notification Event Clubbing, Processing rules.

NOTE 3: The Service Operation (in the case of Event IDs), Bulked Data Formatting and Processing, Data Source, and ADRF information to store data used for generated bulked data, ADRF ID or NWDAF ID (or ADRF Set ID or NWDAF Set ID) storing historical data to be used for bulked data generation can be provided per individual Event ID or Analytics ID included in the Data Specification.

Outputs Required: When the subscription is accepted: Subscription Correlation ID (required for management of the requested subscription). When the subscription is not accepted, an error response.

Outputs, Optional: None.

NOTE 4: When the Target of Event Reporting or Target of Reporting is a SUPI or a GPSI then the subscription may not be accepted, e.g. for user consent is not granted, and an error is sent to the consumer. When the Target of Event Reporting or Target of Reporting is an Internal Group Id, or a list of SUPIs/GPSI(s) or any UE, no error is sent, but a SUPI or GPSI is skipped if user consent is not granted.

7.4.3 Nnwdaf_DataManagement_Unsubscribe service operation

Service operation name: Nnwdaf_DataManagement_Unsubscribe.

Description: The NF consumer deletes an event if already defined in NWDAF.

Inputs, Required: Subscription Correlation ID.

Outputs, Required: Operation execution result indication.

7.4.4 Nnwdaf_DataManagement_Notify service operation

Service operation name: Nnwdaf_DataManagement_Notify.

Description: NWDAF notifies the consumer instance of the requested data or historical analytics which is regarded as a kind of data according to the request.

Inputs, Required: Notification Correlation ID, time stamp.

Inputs, Optional:

- Requested Data or Historical Analytics;
- Fetch Correlation ID;
- Target address where the data or analytics may be retrieved in case the Fetch Correlation ID is included in the notification;
- Unsuccessful bulked data generation;
- Expired bulked data deadline;
- Termination Request: this parameter indicates that NWDAF requests to terminate the data management subscription, i.e. NWDAF will not provide further notifications related to this subscription.

NOTE: The Requested Data or Target address can be provided per Event ID or per Analytics ID specified in the Data Specification field of the subscription. The Requested Historical Analytics or Target address can be provided per analytics ID specified in the Analytics Specification field of the subscription.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

7.4.5 Nnwdaf_DataManagement_Fetch service operation

Service operation name: Nnwdaf_DataManagement_Fetch.

Description: Consumer requests to NWDAF to retrieve the subscribed data or historical analytics which is regarded as a kind of data by such Consumer.

Inputs, Required: Notification Correlation ID, list of Fetch Correlation IDs.

Inputs, Optional: None.

Outputs, Required: Requested data or Historical Aanalytics.

NOTE: The requested data can be provided per Event ID or Analytics ID specified in the Data Specification field of the subscription. The Requested Historical Analytics can be provided per analytics ID specified in the Analytics Specification field of the subscription.

Outputs, Optional: None.

7.5 Nnwdaf_MLModelProvision services

7.5.1 General

Service Description: This service enables the consumer to receive a notification when an ML model matching the subscription parameters becomes available.

When the subscription is accepted by the NWDAF containing MTLF, the consumer NF, i.e. the NWDAF containing Analytics Logical Function, receives from the NWDAF an identifier (Subscription Correlation ID) allowing to further manage (modify, delete) this subscription. The modification of ML model subscription can be enforced by NWDAF based on operator policy and configuration.

7.5.2 Nnwdaf_MLModelProvision_Subscribe service operation

Service operation name: Nnwdaf_MLModelProvision_Subscribe.

Description: Subscribes to NWDAF ML model provision with specific parameters.

Inputs, Required: (set of) Analytics ID(s) defined in Table 7.1-2, Notification Target Address (+ Notification Correlation ID).

Inputs, Optional: Subscription Correlation ID (in the case of modification of the ML model subscription), ML Model Filter Information to indicate the conditions for which ML model for the analytics is requested, and Target of ML Model Reporting to indicate the object(s) for which ML model is requested (e.g. specific UEs, a group of UE(s) or any UE (i.e. all UEs)), ML Model Reporting Information (including e.g. ML Model Target Period), Expiry time.

Outputs Required: When the subscription is accepted: Subscription Correlation ID (required for management of this subscription), Expiry time (required if the subscription can be expired based on the operator's policy).

Outputs, Optional: None.

7.5.3 Nnwdaf_MLModelProvision_Unsubscribe service operation

Service operation name: Nnwdaf_MLModelProvision_Unsubscribe.

Description: unsubscribe to NWDAF ML model provision.

Inputs, Required: Subscription Correlation ID.

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

7.5.4 Nnwdaf_MLModelProvision_Notify service operation

Service operation name: Nnwdaf_MLModelProvision_Notify.

Description: NWDAF notifies the ML model information to the consumer instance which has subscribed to the specific NWDAF service.

Inputs, Required: Set of the tuple (Analytics ID, address (e.g. URL or FQDN) of Model file), Notification Correlation Information.

Inputs, Optional: Validity period, Spatial validity.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

7.6 Nnwdaf_MLModelInfo service

7.6.1 General

Service description: this service enables the consumer to request and get from NWDAF containing MTLF ML Model Information.

7.6.2 Nnwdaf_MLModelInfo_Request service operation

Service operation name: Nnwdaf_MLModelInfo_Request

Description: The consumer requests NWDAF ML Model Information.

Inputs, Required: (Set of) Analytics ID(s) defined in Table 7.1-2.

Inputs, Optional:ML Model Filter Information to indicate the conditions for which ML model for the analytics is requested, and Target of ML Model Reporting to indicate the object(s) for which ML model is requested (e.g. specific UEs, a group of UE(s) or any UE (i.e. all UEs)), ML Model Reporting Information (including e.g. ML Model Target Period).

Outputs, Required: Set of the tuple (Analytics ID, address (e.g. URL or FQDN) of Model file).

Outputs, Optional: Validity period, Spatial validity.

8 DCCF Services

8.1 General

Table 8.1-1 shows the DCCF services and DCCF service operations.

Table 8.1-1: NF services provided by DCCF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Ndccf_DataManagement	Subscribe	Subscribe / Notify	NWDAF, PCF, NSSF, AMF, SMF, NEF, AF
	Unsubscribe		NWDAF, PCF, NSSF, AMF, SMF, NEF, AF
	Notify		NWDAF, PCF, NSSF, AMF, SMF, NEF, AF
	Fetch	Request / Response	NWDAF, PCF, NSSF, AMF, SMF, NEF, AF
Ndccf_ContextManagement	Register	Request / Response	NWDAF, ADRF
	Update	Request / Response	NWDAF, ADRF
	Deregister	Request / Response	NWDAF, ADRF

8.2 Ndccf_DataManagement service

Service Description: This service enables the consumer to subscribe/unsubscribe for data or analytics via the DCCF and have data delivered via the DCCF or via a messaging framework. Historical data, or runtime data may be obtained using this service.

When the subscription is accepted by the DCCF, the consumer NF receives from the DCCF an identifier (Subscription Correlation ID) allowing it to further manage (modify, delete) the subscription.

8.2.2 Ndccf_DataManagement_Subscribe service operation

Service operation name: Ndccf_DataManagement_Subscribe

Description: The consumer NF uses this service operation to subscribe to the DCCF for data or analytics. The subscription includes service operation specific parameters that identify the data or analytics to be provided, and may include formatting and processing instructions that specify how the data is to be delivered to the consumer. The consumer may also request that data shall be stored in an ADRF or an NWDAF hosting ADRF functionality.

Inputs, Required: Service operation, Analytics Specification or Data Specification, Notification Target Address(es) (+ Notification Correlation ID (s)).

Inputs, Optional: Time Window, NF (or NF-Set) ID, ADRF or NWDAF hosting ADRF information, Formatting Instructions, Processing Instructions, user consent check information (i.e. an indication that the data consumer has checked user consent), purpose for data collection.

"Service Operation" identifies the service used by the DCCF to request data or analytics from a Data Source (e.g.: Namf_EventExposure_Subscribe or Nnwdaf_AnalyticsSubscription_Subscribe)

"Analytics Specification or Data Specification" is the "Service Operation" specific required and optional input parameters that identify the data to be collected (e.g. Analytics ID(s) / Event ID (s), Target of Analytics Reporting or Target of Event Reporting, Analytics Filter or Event Filter, etc.). Service Operations and input parameters are defined in clause 7 for NWDAF and in TS 23.502, clause 5.2 for the other NFs.

"Time Window" is the start and stop time when the requested data or analytics was or will be collected. If the Time Window includes a period in the past, then the data or analytics collection is "historical". If the Time Window includes a period in the future, the data or analytics collection is "runtime".

NOTE: Time Window parameter is different from the "Analytics target period" defined in clause 6.1.3.

NF (or NF-Set) ID specifies a data source that may provide the data.

ADRF Information specifies that collected data or analytics is to be stored in an ADRF, and optionally an ADRF or NWDAF ID.

Formatting Instructions and Processing Instructions are as defined in clause 5A.4.

Outputs Required: When the subscription is accepted: Subscription Correlation ID (required for management of this subscription).

Outputs, Optional: First corresponding event report is included, if available (see clause 4.15.1 ofTS 23.502 [3]), Requested data.

8.2.3 Ndccf_DataManagement_Unsubscribe service operation

Service operation name: Ndccf_DataManagement_Unsubscribe

Description: The consumer unsubscribes to DCCF for data or analytics.

Inputs, Required: Subscription Correlation ID.

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

8.2.4 Ndccf_DataManagement_Notify service operation

Service operation name: Ndccf_DataManagement_Notify

Description: Provides the previously subscribed Data or Analytics, or notification of availability of previously subscribed Data or Analytics to the NF Consumer when data delivery is via the DCCF.

Inputs, Required: Notification Correlation Information.

Inputs, Optional: Data or Analytics, Fetch Instructions

Fetch Instructions indicate whether the data or analytics are to be fetched by the Consumer. If the data or analytics are to be fetched, the fetch instructions include an address from which the data may be fetched and one or more Fetch Correlation IDs.

NOTE: Data or Analytics provided in notifications are processed and formatted according to the Processing and Formatting Instructions provided by the Consumer in Ndccf_DataManagement_Subscribe.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

8.2.5 Ndccf_DataManagement_Fetch service operation

Service operation name: Ndccf_DataManagement_Fetch

Description: Consumer retrieves from the DCCF data previously subscribed to by the Consumer, as indicated by Fetch Instructions received in Ndccf_DataManagement_Notify.

Inputs, Required: Set of Fetch Correlation ID(s).

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: Formatted /Processed Events or Analytics.

8.3 Ndccf_ContextManagement service

8.3.1 General

Service Description: This service enables the consumer to register collected data or analytics with the DCCF.

When the DCCF is configured by the consumer NF, the DCCF supplies a Transaction Reference Id. The Consumer NF may use the Transaction Reference Id in subsequent transactions to update or delate the context in the DCCF.

8.3.2 Ndccf_ContextManagement_Register service operation

Service operation name: Ndccf_ContextManagement_Register

Description: The consumer NF uses this service operation to register data or analytics it is collecting to the DCCF. The registration includes a service operation specific Analytics/Data Specification that identifies the data or analytics that are being collected or has been collected.

Inputs, Required: Service Operation, Analytics/Data Specification, NWDAF ID or ADRF ID.

Inputs, Optional: None

NOTE: The input parameters are defined as:

- "Service Operation" identifies the service used to collect the data or analytics from a Data Source (e.g. Namf_EventExposure_Subscribe or Nnwdaf_AnalyticsSubscription_Subscribe).
- "Analytics/Data Specification" is the "Service Operation" specific required and optional input parameters that identify the collected data (i.e. Analytics ID(s) / Event ID (s), Target of Analytics Reporting or Target of Event Reporting, Analytics Filter or Event Filter, etc.). NF Service Operations and input parameters are defined in clause 7 and clause 5.2 of TS 23.502 [3].
- NWDAF ID or ADRF ID specify the ADRF or NWDAF with the stored data.

Outputs Required: Transaction Reference ID(s), Operation execution result indication.

Outputs, Optional: None.

8.3.3 Ndccf_ContextManagement_Update service operation

Service operation name: Ndccf_ContextManagement_Update

Description: The consumer NF uses this service operation to update a registration of data or analytics to the DCCF. The registration update includes a service operation specific Analytics/Data Specification that identifies the data or analytics that is being collected or has been collected.

Inputs, Required: Transaction Reference ID(s), Service Operation, Analytics/Data Specification

Inputs, Optional: None

NOTE: The input parameters are defined in clause 8.3.2.

Outputs Required: Transaction Reference ID(s), Operation execution result indication.

8.3.4 Ndccf_ContextManagement_Deregister service operation

Service operation name: Ndccf_ContextManagement_Deregister

Description: The consumer NF uses this service operation to delete a registration of data or analytics to the DCCF.

Inputs, Required: Transaction Reference ID(s)

Inputs, Optional: None

Outputs Required: Transaction Reference ID(s), Operation execution result indication.

Outputs, Optional: None.

9 MFAF Services

9.1 General

Table 9.1-1 shows the MFAF services and MFAF service operations.

Table 9.1-1: NF services provided by MFAF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nmfaf_3daDataManagement	Configure	Request / Response	DCCF
	Deconfigure	Request / Response	DCCF
Nmfaf_3caDataManagement	Notify	Subscribe / Notify	NWDAF, PCF, NSSF, AMF, SMF, NEF, AF
	Fetch	Request / Response	NWDAF, PCF, NSSF, AMF, SMF, NEF, AF

9.2 Nmfaf_3daDataManagement service

9.2.1 General

Service Description: The consumer (e.g. DCCF) uses this service to instruct the MFAF to map data or analytics received by the MFAF to out-bound notification endpoints. Configuration of the MFAF by the consumer may include

formatting and processing instructions for each notification endpoint as described in clause 5A.4. The sending of historical data or run-time data may be configured/deconfigured using this service.

When the MFAF is configured by the consumer NF, the MFAF provides a Transaction Reference Id. The Consumer NF may use the Transaction Reference Id in subsequent transactions to modify or remove (deconfigure) the sending of data to consumers.

9.2.2 Nmfaf_3daDataManagement_Configure service operation

Service operation name: Nmfaf_3daDataManagement_Configure

Description: The consumer configures or reconfigures the MFAF to map data or analytics received by the MFAF to out-bound notification endpoints and to format and process the out-bound data or analytics.

Inputs, Required: Data Consumer or Analytics Consumer Information.

"Data Consumer or Analytics Consumer Information" contains for each notification endpoint, the consumer provided Notification Target Address (+ Analytics Consumer Notification Correlation ID) or other endpoint addresses if provisioned on the DCCF to be used by the MFAF when sending notifications.

Inputs, Optional: Formatting Instructions, Processing Instructions, MFAF Notification Information, Transaction Reference Id, ADRF ID.

"MFAF Notification Information" is used to identify Event Notifications received from a Data Source and comprises the MFAF Notification Target Address (+ MFAF Notification Correlation ID). If a Data Source is already supplying the data to the MFAF, the MFAF Notification Information previously provided by the MFAF and used by the DCCF to obtain data from a Data Source is provided as an Input. If a new subscription to a Data Source is needed, the MFAF Notification Information is not specified as an Input and the MFAF provides Notification Information as an output. The MFAF Notification Information may subsequently be used by the DCCF when subscribing to a Data Source.

Outputs Required: Operation execution result indication.

Outputs, Optional: MFAF Notification Information, Transaction Reference Id.

9.2.3 Nmfaf_3daDataManagement_Deconfigure service operation

Service operation name: Nmfaf_3daDataManagement_Deconfigure

Description: Description: The consumer configures the MFAF to stop mapping data or analytics received by the MFAF to one or more out-bound notification endpoints.

Inputs, Required: Data Consumer or Analytics Consumer Information, Transaction Reference Id.

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

9.3 Nmfaf_3caDataManagement service

9.3.1 General

Service Description: This service is used to supply data or analytics from the MFAF to notification endpoints. Notifications may contain data or analytics, or an indication of availability of data or analytics.

9.3.2 Nmfaf_3caDataManagement_Notify service operation

Service operation name: Nmfaf_3caDataManagement_Notify

Description: Provides data or analytics or notification of availability of data or analytics to notification endpoints.

Inputs, Required: Notification Correlation Information.

Inputs, Optional: Data or Analytics, Fetch Instructions.

Fetch Instructions indicate whether the data or analytics are to be fetched by the Consumer. If the data or analytics are to be fetched, the fetch instructions include an address from which the data may be fetched and one or more Fetch Correlation IDs.

NOTE: Data or Analytics provided in notifications can be processed and formatted according to the Processing and Formatting Instructions provided by the Consumer.

Outputs, Required: None.

Outputs, Optional: None.

9.3.3 Nmfaf_3caDataManagement_Fetch service operation

Service operation name: Nmfaf_3caDataManagement_Fetch

Description: Consumer retrieves data or analytics from the MFAF as indicated by Nmfaf_3caDataManagement_Notify Fetch Instruction.

Inputs, Required: Set of Fetch Correlation ID(s).

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: Data or Analytics.

NOTE: Data or Analytics provided in notifications can be processed and formatted according to the Processing and Formatting Instructions provided by the Consumer.

10 ADRF Services

10.1 General

Table 10.1-1 shows the ADRF services and ADRF service operations.

ADRF service operations may be used to store data or analytics in the ADRF, retrieve data or analytics from an ADRF, or delete data or analytics from an ADRF.

NOTE: Storage of ML models in ADRF is not specified in this Release of the specification.

Table 10.1-1: NF services provided by ADRF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nadrf_DataManagement	StorageRequest	Request / Response	DCCF, NWDAF
	StorageSubscriptionRequest	Request / Response	DCCF, NWDAF
	StorageSubscriptionRemoval	Request / Response	DCCF, NWDAF
	RetrievalRequest	Request / Response	DCCF, NWDAF
	RetrievalSubscribe	Subscribe / Notify	DCCF, NWDAF
	RetrievalUnsubscribe		DCCF, NWDAF
	RetrievalNotify		DCCF, NWDAF
	Delete	Request / Response	DCCF, NWDAF

10.2 Nadrf_DataManagement service

10.2.1 General

Service Description: This service enables the consumer to store, retrieve, and remove data or analytics from an ADRF.

10.2.2 Nadrf_DataManagement_StorageRequest service operation

Service operation name: Nadrf_DataManagement_StorageRequest

Description: The consumer NF uses this service operation to request the ADRF to store data or analytics. Data or analytics are provided to the ADRF in the request message.

Inputs, Required: Data or Analytics to be stored.

Inputs, Optional: None.

Outputs Required: Result Indication.

Outputs, Optional: Storage Transaction Identifier.

10.2.3 Nadrf_DataManagement_StorageSubscriptionRequest service operation

Service operation name: Nadrf_DataManagement_StorageSubscriptionRequest

Description: The consumer (NWDAF or DCCF) uses this service operation to request the ADRF to initiate a subscription for data or analytics (see clause 6.2B.3). Data or analytics provided in notifications as a result of the subsequent subscription by the ADRF are stored in the ADRF.

This service operation provides parameters needed by the ADRF to initiate the subscription (to a DCCF or NWDAF).

Inputs, Required: Service operation, Analytics Specification or Data Specification, Target NF (or Set) to subscribe to for notifications.

"Service Operation" identifies the service used to request data or analytics from a Data Source (e.g. Namf_EventExposure_Subscribe or Nnwdaf_AnalyticsSubscription_Subscribe)

"Analytics Specification or Data Specification" is the "Service Operation" specific required and optional input parameters that identify the data to be collected (e.g. Analytics ID(s) / Event ID (s), Target of Analytics Reporting or Target of Event Reporting, Analytics Filter or Event Filter, etc.). Service Operations and input parameters are defined in clause 7 for NWDAF and in TS 23.502 [3], clause 5.2 for the other NFs.

"Target NF (or Set) to subscribe to for notifications" may be a DCCF or NWDAF that can provide the data or analytics

Inputs, Optional: Formatting Instructions, Processing Instructions.

Formatting Instructions and Processing Instructions are as defined in clause 5A.4.

Outputs Required: Transaction Reference ID.

Outputs, Optional: None.

10.2.4 Nadrf_DataManagement_StorageSubscriptionRemoval service operation

Service operation name: Nadrf_DataManagement_StorageSubscriptionRemoval

Description: The consumer NF uses this service operation to request that the ADRF no longer subscribes to data or analytics it is collecting and storing.

Inputs, Required: Transaction Reference ID provided in the Nadrf_DataManagement_StorageSubscriptionRequest Output.

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

10.2.5 Nadrf_DataManagement_RetrievalRequest service operation

Service operation name: Nadrf_DataManagement_RetrievalRequest

Description: The consumer NF uses this service operation to retrieve stored data or analytics from the ADRF. The Nadrf_DataManagement_RetrievalRequest response either contains the data or analytics, or provides instructions for fetching the data or analytics. The Nadrf_DataManagement_RetrievalRequest may be unsolicited or sent in response to a Fetch Instructions from the ADRF in an Nadrf_DataManagement_RetrievalNotify.

Inputs, Required: one of the following:

- Storage Transaction Identifier;
- Service Operation, Analytics Specification or Data Specification and Time Window; or
- Fetch Correlation ID(s) if the RetrievalRequest is in response to a Fetch Instruction.

"Service Operation" identifies the service used to obtain the data or analytics from a Data Source (e.g. Namf_EventExposure_Subscribe or Nnwdaf_AnalyticsSubscription_Subscribe).

"Analytics Specification or Data Specification" is the "Service Operation" specific required and optional input parameters that identify the data that was stored (e.g. Analytics ID(s) / Event ID (s), Target of Analytics Reporting or Target of Event Reporting, Analytics Filter or Event Filter, etc.). Service Operations and input parameters are defined in clause 7 for NWDAF and in TS 23.502 [3], clause 5.2 for the other NFs.

"Time Window" is the start and stop time when the requested data or analytics was collected.

Inputs, Optional: None.

Outputs Required: Result Indication.

Outputs, Optional: Data or Analytics.

10.2.6 Nadrf_DataManagement_RetrievalSubscribe service operation

Service operation name: Nadrf_DataManagement_RetrievalSubscribe

Description: The consumer NF uses this service operation to retrieve stored data or analytics from the ADRF and to receive future notifications containing the corresponding data or analytics received by ADRF.

Inputs, Required: Service Operation, Analytics Specification or Data Specification, Time Window.

"Service Operation" identifies the service used to obtain the data or analytics from a Data Source (e.g. Namf_EventExposure_Subscribe or Nnwdaf_AnalyticsSubscription_Subscribe).

"Analytics Specification or Data Specification" is the "Service Operation" specific required and optional input parameters that identify the data that was stored (e.g. Analytics ID(s) / Event ID (s), Target of Analytics Reporting or Target of Event Reporting, Analytics Filter or Event Filter, etc.). Service Operations and input parameters are defined in clause 7 for NWDAF and in TS 23.502 [3], clause 5.2 for the other NFs.

"Time Window" is the start and stop time when the requested data or analytics was collected. If Time Window includes a period in the future, subsequent notifications containing the requested data or analytics received by the ADRF are sent to the notification endpoint.

Inputs, Optional: None.

Outputs Required: Result Indication.

Outputs, Optional: Subscription Correlation ID.

10.2.7 Nadrf_DataManagement_RetrievalUnsubscribe service operation

Service operation name: Nadrf_DataManagement_RetrievalUnsubscribe

Description: The consumer NF uses this service operation to request that the ADRF no longer sends data or analytics to a notification endpoint.

Inputs, Required: Subscription Correlation ID.

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

10.2.8 Nadrf_DataManagement_RetrievalNotify service operation

Service operation name: Nadrf_DataManagement_RetrievalNotify

Description: This service operation provides consumers with either data or analytics from an ADRF, or instructions to fetch the data or analytics from an ADRF. The notifications are provided to consumers that have subscribed using the Nadrf_DataManagement_RetrievalSubscribe service operation. Historical data or analytics may be retrieved from ADRF storage and data received in the future be sent when obtained by the ADRF.

Inputs, Required: Notification Correlation Information.

Inputs, Optional: Data or Analytics, Fetch Instructions.

Fetch Instructions indicate whether the data or analytics are to be fetched from the ADRF by the Consumer. If the data or analytics are to be fetched, the fetch instructions include an address from which the data may be fetched and one or more Fetch Correlation IDs. Data or Analytics are fetched using the Nadrf_DataManagement_RetrievalRequest service operation.

NOTE: Data or Analytics provided in notifications from the DCCF are processed and formatted according to the Processing and Formatting Instructions provided by the Consumer in Ndccf_DataManagement_Subscribe.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

10.2.9 Nadrf_DataManagement_Delete

Service operation name: Nadrf_DataManagement_Delete

Description: This service operation instructs the ADRF to delete stored data.

Inputs, Required: One of the following:

- Storage Transaction Identifier; or
- Service Operation, Analytics Specification or Data Specification and Time Window.

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-05	SP#84	SP-190456	-	-	-	MCC Editorial update for presentation to TSG SA#84 for approval	1.0.0
2019-06	SP#84	-	-	-	-	MCC editorial update for publication after approval at TSG SA#84	16.0.0
2019-09	SP#85	SP-190612	0001	3	F	Clarifications to Observed Service experience related network data analytics	16.1.0
2019-09	SP#85	SP-190612	0010	1	F	Specification clean-up	16.1.0
2019-09	SP#85	SP-190612	0012	3	F	Miscellaneous corrections to TS 23.288	16.1.0
2019-09	SP#85	SP-190612	0014	1	F	Clarification of NF and AF	16.1.0
2019-09	SP#85	SP-190612	0015	3	F	Update the Analytics information provided by NWDAF	16.1.0
2019-09	SP#85	SP-190612	0017	2	F	Closing open issue on NEF-AF interaction for data collection from AF	16.1.0
2019-09	SP#85	SP-190612	0026	1	F	Clarification of the correlation information	16.1.0
2019-09	SP#85	SP-190612	0027	4	F	Clarifications of the pre-check behaviours of the NF	16.1.0
2019-09	SP#85	SP-190612	0029	3	F	Corrections to slice load level analytics	16.1.0
2019-09	SP#85	SP-190612	0034	3	F	Clarifications on Potential QoS Change	16.1.0
2019-09	SP#85	SP-190612	0036	1	F	CR to properly separate UE identifiers from Analytics Filter	16.1.0
2019-09	SP#85	SP-190612	0037	1	F	CR for update of observed service experience	16.1.0
2019-09	SP#85	SP-190612	0039	3	F	Miscellaneous editorial corrections	16.1.0
2019-09	SP#85	SP-190612	0040	3	F	Optionality of data to be collected by NWDAF	16.1.0
2019-09	SP#85	SP-190612	0042	1	F	Clarification on Data Collection	16.1.0
2019-09	SP#85	SP-190612	0045	1	F	Probability assertion clarification on NWDAF services description	16.1.0
2019-09	SP#85	SP-190612	0046	1	F	Corrections for analytics exposure framework related parameters	16.1.0
2019-09	SP#85	SP-190612	0052	1	F	BSF and PCF selection for data collection	16.1.0
2019-09	SP#85	SP-190612	0054	-	F	Corrections to Nnwdaf_AnalyticsSubscription_Subscribe and Nnwdaf_AnalyticsInfo_Request service operations	16.1.0
2019-12	SP#86	SP-191079	0002	6	F	Clarifications to NF load data analytics	16.2.0
2019-12	SP#86	SP-191079	0003	8	F	Clarifications to Network Performance related network data analytics	16.2.0
2019-12	SP#86	SP-191079	0004	3	F	Clarifications to Abnormal behaviour analytics	16.2.0
2019-12	SP#86	SP-191079	0009	4	F	Clarifications to UE mobility and Abnormal behaviour analytics	16.2.0
2019-12	SP#86	SP-191079	0043	2	F	Remove UE related analytics for any UE	16.2.0
2019-12	SP#86	SP-191079	0044	6	F	Clarifications to UE communication and mobility analytics output	16.2.0
2019-12	SP#86	SP-191079	0047	3	F	Corrections for observed Service experience related network data analytics	16.2.0
2019-12	SP#86	SP-191079	0055	01	F	Terminology Alignment	16.2.0
2019-12	SP#86	SP-191079	0057	5	F	Editor's Notes cleanup	16.2.0
2019-12	SP#86	SP-191079	0062	-	F	Corrections to User Data Congestion Analytics	16.2.0
2019-12	SP#86	SP-191079	0063	-	F	Correction for data collection from OAM	16.2.0
2019-12	SP#86	SP-191079	0064	7	F	Corrections to general and framework parts of analytics	16.2.0
2019-12	SP#86	SP-191079	0065	-	F	Corrections to data collection from NFs	16.2.0
2019-12	SP#86	SP-191079	0066	6	F	Miscellaneous corrections/updates to TS 23.288	16.2.0
2019-12	SP#86	SP-191079	0068	4	F	Clarification of the data collection of the OSE	16.2.0
2019-12	SP#86	SP-191079	0071	3	F	Update to UE related analytics	16.2.0
2019-12	SP#86	SP-191079	0072		F	Clarifications on Supporting Modification of Analytics Subscription	16.2.0
2019-12	SP#86	SP-191079	0076	2	F	Removing Editor's note on how to find a PCF instance serving a UE	16.2.0
2019-12	SP#86	SP-191079	0078	2	F	User Data Congestion - Removal of Editor's Notes and Description Alignments	16.2.0
2019-12	SP#86	SP-191079	0081	3	F	CR to update UE communication	16.2.0
2019-12	SP#86	SP-191079	0084	3	F	Correction to Analytics Filter for slice load level analytics	16.2.0
2019-12	SP#86	SP-191079	0087	3	F	Clarification on NWDAF-assisted expected UE behavioural analytics	16.2.0
2019-12	SP#86	SP-191079	0088		F	Update the correlation information for AMF data and RAN data	16.2.0
2019-12	SP#86	SP-191079	0091	1	F	Clarification of UE related analytics	16.2.0
2019-12	SP#86	SP-191079	0092		F	Clarification of QoS requirements parameter used for QoS Sustainability Analytics	16.2.0
2019-12	SP#86	SP-191079	0093	4	F	Alignments on Analytics Filter Information and clarifications on Reporting Thresholds	16.2.0
2019-12	SP#86	SP-191079	0094	1	F	Clarification for UPF related data collection	16.2.0
2019-12	SP#86	SP-191120	0095	3	F	Alignment of User Data Congestion Analytics	16.2.0
2019-12	SP#86	SP-191079	0099	1	F	NEF parameter mapping for outbound analytics	16.2.0
2019-12	SP#86	SP-191079	0100	5	F	Alignments on QoS Sustainability Analytics	16.2.0
2020-03	SP#87E	SP-200070	0103	1	F	Clarification on definitions and NSI	16.3.0

2020-03	SP#87E	SP-200070	0104	-	F	NWDAF collect MDT/SON parameters	16.3.0
2020-03	SP#87E	SP-200070	0105	1	F	Update to Clause 6.1.3 Contents of Analytics Exposure	16.3.0
2020-03	SP#87E	SP-200070	0108	2	F	CR to update Observed Service Experience	16.3.0
2020-03	SP#87E	SP-200070	0109	3	F	Corrections on UE mobility analytics type by NWDAF service	16.3.0
2020-03	SP#87E	SP-200070	0110	3	F	Corrections on UE mobility analytics type by NWDAF service	16.3.0
2020-03	SP#87E	SP-200070	0112	2	F	Correct the filters for UE related analytics	16.3.0
2020-03	SP#87E	SP-200070	0113	4	F	A mechanism to avoid the flooding of reporting	16.3.0
2020-03	SP#87E	SP-200070	0114	1	F	Reporting information updates	16.3.0
2020-03	SP#87E	SP-200070	0115	1	F	Mega CR on editorial corrections	16.3.0
2020-03	SP#87E	SP-200070	0117	1	F	Slice service experience data collection corrections	16.3.0
2020-03	SP#87E	SP-200070	0119	1	F	Add the definition for Maximum number of results parameter into clause 6.1.3	16.3.0
2020-03	SP#87E	SP-200070	0123	1	F	Clarification of clause 6.7.2 UE mobility analytics	16.3.0
2020-03	SP#87E	SP-200070	0124	1	F	Clarification of clause 6.7.4 Expected UE behavioural parameters related network data analytics	16.3.0
2020-03	SP#87E	SP-200070	0126	1	F	Clarification on abnormal behaviour analytics	16.3.0
2020-03	SP#87E	SP-200070	0127	1	F	Clarifications on data collection	16.3.0
2020-03	SP#87E	SP-200070	0128	1	F	Corrections to Observed Service Experience analytics	16.3.0
2020-03	SP#87E	SP-200070	0129	1	F	Corrections to User Data Congestion Analytics	16.3.0
2020-03	SP#87E	SP-200070	0130	-	F	Corrections related to Analytics Filter Information and others	16.3.0
2020-03	SP#87E	SP-200070	0132	-	F	Clarifications on Inputs of NWDAF Analytics Subscription	16.3.0
2020-03	SP#87E	SP-200070	0139	-	F	Clarification of data collection from UPF	16.3.0
2020-03	SP#87E	SP-200070	0140	-	F	TS 23.288 editor's note handling	16.3.0
2020-03	SP#87E	SP-200070	0142	1	F	Clarification on the NWDAF services invoked in Abnormal behaviour	16.3.0
2020-07	SP#88E	SP-200431	0118	3	F	Abnormal analytics for any UE	16.4.0
2020-07	SP#88E	SP-200431	0146	1	F	Clarification of NF load analytics procedure	16.4.0
2020-07	SP#88E	SP-200431	0148	1	F	Clarification on Data Collection Procedure	16.4.0
2020-07	SP#88E	SP-200431	0149	1	F	Correction on Probability Assertion	16.4.0
2020-07	SP#88E	SP-200431	0150	1	F	Miscellaneous FASMO corrections to service experience analytics	16.4.0
2020-07	SP#88E	SP-200431	0153	1	F	Support of abnormal behaviour analytics for any UE	16.4.0
2020-07	SP#88E	SP-200431	0154	1	F	Support of data collection for any UE	16.4.0
2020-07	SP#88E	SP-200431	0155	2	F	Clarification on UE mobility analytics exposed to AF	16.4.0
2020-07	SP#88E	SP-200431	0156	1	F	Abnormal analytics clarifications (not any UE related)	16.4.0
2020-07	SP#88E	SP-200431	0158	1	F	Clarification on Event and Analytics Filters for some analytics types	16.4.0
2020-07	SP#88E	SP-200431	0159	-	F	The term MoS to apply for all kind of services	16.4.0
2020-07	SP#88E	SP-200431	0160	1	F	Further corrections to Observed Service Experience analytics	16.4.0
2020-07	SP#88E	SP-200431	0161	1	F	Clarifications on procedures for analytics exposure	16.4.0
2020-07	SP#88E	SP-200431	0162	1	F	Clarifications on procedures for data collection	16.4.0
2020-07	SP#88E	SP-200431	0163	1	F	Further clarifications on abnormal behaviour related network data analytics	16.4.0
2020-07	SP#88E	SP-200431	0165	1	F	Clarification for the Network Performance analytics	16.4.0
2020-07	SP#88E	SP-200431	0166	1	F	Updates of data collection for slice service experience	16.4.0
2020-07	SP#88E	SP-200431	0167	1	F	Corrections related to external UE ID	16.4.0
2020-07	SP#88E	SP-200431	0168	-	F	General clean-up for output abnormal behaviour analytics	16.4.0
2020-07	SP#88E	SP-200431	0169	-	F	Removing service provider actions for exception ID ping-ponging across neighbouring cells	16.4.0
2020-07	SP#88E	SP-200431	0170	1	F	Updated Event IDs for analytics	16.4.0
2020-07	SP#88E	SP-200431	0172	1	F	Corrections to Nnwdaf service operations	16.4.0
2020-07	SP#88E	SP-200431	0173	1	F	Adding UDM and OAM as consumers of services provided by NWDAF	16.4.0
2020-07	SP#88E	SP-200431	0176	1	F	Corrections for maximum number of objects and Maximum number of SUPIs	16.4.0
2020-09	SP#89E	SP-200679	0177	1	F	Service experience analytics discrimination	16.5.0
2020-09	SP#89E	SP-200679	0178	-	F	Corrections for wrong references for TS 28.532 clauses	16.5.0
2020-09	SP#89E	SP-200679	0179	-	F	Clarification on Target of Event Reporting	16.5.0
2020-09	SP#89E	SP-200679	0181	2	F	Clarification on Analytics Exposure	16.5.0
2020-09	SP#89E	SP-200679	0182	1	F	Clarification on data collection for statistics	16.5.0
2020-09	SP#89E	SP-200679	0183	1	F	Clarification on mapping of expected analytics type and Exception IDs	16.5.0
2020-09	SP#89E	SP-200679	0184	1	F	Clarification on NWDAF identifying the AF to collect data for an Event	16.5.0
2020-09	SP#89E	SP-200679	0186	1	F	Clarification on Multiple Parameter Sets for QoS Sustainability	16.5.0
2020-12	SP#90E	SP-200957	0188	1	F	Clarifications for Charging function as NWDAF consumer	16.6.0
2021-03	SP#90E	SP-210246	0192	-	F	Correct wrong reference	16.7.0
2021-03	SP#90E	SP-210246	0199	1	F	UE location in the AMF	16.7.0
2021-03	SP#90E	SP-210070	0193	1	B	Analytics ID UE communication and Observed Service Experience Extension to Support Application Related Analytics for RFSP Policy	**17.0.0**
2021-03	SP#90E	SP-210070	0194	2	B	Dispersion Analytics	**17.0.0**
2021-03	SP#90E	SP-210070	0195	1	B	Persistent Data Collection	**17.0.0**

2021-03	SP#90E	SP-210070	0196	1	C	Extending Observed Service Experience related network data analytics with cell energy saving state to Support UP path selection enhancement	**17.0.0**
2021-03	SP#90E	SP-210070	0197	1	B	Adding a new analytics WLAN performance	**17.0.0**
2021-03	SP#90E	SP-210070	0198	1	B	Adding Analytics IDs	**17.0.0**
2021-03	SP#90E	SP-210070	0200	1	B	Extensions to User Data Congestion Analytics	**17.0.0**
2021-03	SP#90E	SP-210070	0201	1	C	KI#4: Slice load level related network data analytics	**17.0.0**
2021-03	SP#90E	SP-210070	0202	1	C	KI#4: Additional consumer NFs for service experience analytics	**17.0.0**
2021-03	SP#90E	SP-210070	0203	1	C	Network slice information from OAM	**17.0.0**
2021-03	SP#90E	SP-210070	0204	1	C	UE Communication analytics updates for user plane optimization	**17.0.0**
2021-03	SP#90E	SP-210070	0205	1	B	NWDAF decomposition	**17.0.0**
2021-03	SP#90E	SP-210070	0206	1	B	NWDAF - Data repository function	**17.0.0**
2021-03	SP#90E	SP-210070	0207	1	B	Procedure for Multiple NWDAF Analytics aggregation	**17.0.0**
2021-03	SP#90E	SP-210070	0208	1	B	Procedure for time coordination across multiple NWDAF instances	**17.0.0**
2021-03	SP#90E	SP-210070	0209	1	B	NF Load analytics enhancement	**17.0.0**
2021-03	SP#90E	SP-210070	0210	1	B	Session Management Congestion Control Experience Analytics	**17.0.0**
2021-03	SP#90E	SP-210070	0211	1	B	Adding the new analytics Redundant Transmission Experience	**17.0.0**
2021-03	SP#90E	SP-210070	0212	1	C	Extension of the existing analytics, UE Mobility	**17.0.0**
2021-03	SP#90E	SP-210070	0213	1	B	Hierarchical Principles and Interactions on Multiple NWDAFs in TS23.288	**17.0.0**
2021-03	SP#90E	SP-210070	0214	1	B	Principles, Procedures, Services of Bulked Data Collection in TS23.288	**17.0.0**
2021-03	SP#90E	SP-210071	0215	1	B	Implementation of Support For Discovering and Tracking Entities in Area of Interesting in TS23.288	**17.0.0**
2021-03	SP#90E	SP-210071	0216	1	B	Implementation of Enhancements on Event Exposure used by NWDAF in TS23.288	**17.0.0**
2021-03	SP#90E	SP-210071	0218	1	B	ML model sharing between NWDAF instances	**17.0.0**
2021-03	SP#90E	SP-210071	0219	1	B	Analytics ID Service Experience Extension to Support UP path selection enhancement	**17.0.0**
2021-03	SP#90E	SP-210071	0220	1	B	KI#11: Update of data collection procedures	**17.0.0**
2021-03	SP#90E	SP-210071	0221	1	B	KI#1: Extension of functional descriptions for Model training logical function	**17.0.0**
2021-03	SP#90E	SP-210071	0222	1	B	KI#19: Procedures for ML model provisioning and training	**17.0.0**
2021-03	SP#90E	SP-210071	0223	1	B	Multiple NWDAF instances architecture	**17.0.0**
2021-03	SP#90E	SP-210071	0224	1	B	Procedures for model sharing	**17.0.0**
2021-03	SP#90E	SP-210071	0229	1	B	NWDAF discovery for no AOI case	**17.0.0**
2021-03	SP#90E	SP-210071	0230	1	B	Support of analytics aggregation without provision of AOI	**17.0.0**
2021-03	SP#90E	SP-210071	0233	1	B	Support of DN performance analytics by NWDAF	**17.0.0**
2021-03	SP#90E	SP-210071	0235	1	B	DCCF and ADRF architectural changes to increasing efficiency of data collection	**17.0.0**
2021-03	SP#90E	SP-210071	0236	1	B	Procedures for data collection using DCCF	**17.0.0**
2021-03	SP#90E	SP-210071	0237	1	B	Procedures for data collection using DCCF and Messaging Framework	**17.0.0**
2021-03	SP#90E	SP-210071	0238	-	B	Procedures for analytics exposure using DCCF	**17.0.0**
2021-03	SP#90E	SP-210071	0239	1	B	Procedures for analytics exposure using DCCF and Messaging Framework	**17.0.0**
2021-03	SP#90E	SP-210071	0240	-	B	NWDAF usage of partitioning criteria	**17.0.0**
2021-03	SP#90E	SP-210071	0241	1	B	New procedure for data collection from UE	**17.0.0**
2021-03	SP#90E	SP-210071	0244	1	B	Increasing efficiency of data collection (Architecture part)	**17.0.0**
2021-03	SP#90E	SP-210071	0248	1	B	Update the procedure for Observed Service Experience related network data analytics case	**17.0.0**
2021-03	SP#90E	SP-210072	0250	1	B	Service operations for Multiple NWDAF Analytics aggregation	**17.0.0**
2021-03	SP#90E	SP-210072	0251	1	B	NWDAF Reselection for Multiple NWDAF deployments - procedures	**17.0.0**
2021-03	SP#90E	SP-210072	0252	1	B	NWDAF Discovery and Selection for Multiple NWDAF	**17.0.0**
2021-03	SP#90E	SP-210072	0255	1	B	Improvements on analytics subsets, accuracy levels, and ordering of results	**17.0.0**
2021-03	SP#90E	SP-210072	0256	1	B	NWDAF Reselection for Multiple NWDAF deployments - service operations	**17.0.0**
2021-06	SP#92E	SP-210348	0243	5	B	Exposing UE mobility analytics for multiple NWDAFs case	17.1.0
2021-06	SP#92E	SP-210348	0257	1	B	KI#7 - Extensions to User Data Congestion Analytics	17.1.0
2021-06	SP#92E	SP-210348	0258	3	B	KI#8 - Resolving Editors note on mapping UE IP address and SUPI or GPSI	17.1.0
2021-06	SP#92E	SP-210348	0259	2	B	NWDAF registering into UDM	17.1.0
2021-06	SP#92E	SP-210348	0260	2	B	Updating clause 5.2 for the discovery of NWDAFs	17.1.0
2021-06	SP#92E	SP-210348	0262	2	B	CR to update MTLF services to resolve ENs	17.1.0
2021-06	SP#92E	SP-210348	0263	1	B	CR to resolve ENs related to multiple MTLFs	17.1.0
2021-06	SP#92E	SP-210330	0265	1	A	Delete NSI ID via N7 interface	17.1.0
2021-06	SP#92E	SP-210350	0266	1	F	Clarification on DCCF usage in non-roaming architecture	17.1.0
2021-06	SP#92E	SP-210350	0267	1	F	Clarification on applying analytics subsets	17.1.0
2021-06	SP#92E	SP-210348	0268	1	B	Adding Application Status to analytics filter information	17.1.0
2021-06	SP#92E	SP-210350	0272	1	D	Removal of Editorial Note related to Namf/Nsmf_EventExposure	17.1.0

2021-06	SP#92E	SP-210348	0273	1	B	Preferred granularity of location in analytics outputs	17.1.0
2021-06	SP#92E	SP-210348	0274	1	B	Alignments on analytics subsets, accuracy levels, and ordering of results	17.1.0
2021-06	SP#92E	SP-210348	0275	1	B	Use of UE behaviour, location and communication trends for analytics optimization	17.1.0
2021-06	SP#92E	SP-210348	0276	1	B	Service Experience Analytics outputs RAT Type and Frequency information	17.1.0
2021-06	SP#92E	SP-210350	0278	-	F	Removal of analytics consumer or data consumer from the list	17.1.0
2021-06	SP#92E	SP-210350	0280	3	F	Resolving EN on analytics metadata request	17.1.0
2021-06	SP#92E	SP-210350	0282	-	F	Analytics Context Information Transfer	17.1.0
2021-06	SP#92E	SP-210350	0283	1	F	Services for Analytics Subscription Transfer	17.1.0
2021-06	SP#92E	SP-210348	0285	1	B	Removing EN on dataset statistical properties related to analytics aggregation definitions.	17.1.0
2021-06	SP#92E	SP-210350	0286	4	F	Removing EN on bulked data definitions and procedures.	17.1.0
2021-06	SP#92E	SP-210348	0287	1	B	Remove ENs from Event Muting Mechanisms	17.1.0
2021-06	SP#92E	SP-210348	0288	1	B	Removal of FFS on SMF mapping of PDU sessions to TAI	17.1.0
2021-06	SP#92E	SP-210348	0289	2	B	Removal of EN related to network slice association information in TS 23.288.	17.1.0
2021-06	SP#92E	SP-210348	0290	1	B	Alignment of NWDAF discovery of data exposure capability in TS 23.288.	17.1.0
2021-06	SP#92E	SP-210348	0291	4	B	NWDAF discovery and selection based on ML model information	17.1.0
2021-06	SP#92E	SP-210348	0293	4	B	Add bandwidth into Dispersion analytics per slice	17.1.0
2021-06	SP#92E	SP-210350	0295	1	C	Improve the accuracy of the analytics ouput based on Abnormal Behaviour analytics interactions between NWDAFs	17.1.0
2021-06	SP#92E	SP-210348	0297	1	B	Clarification on MTLF determining when further training is required	17.1.0
2021-06	SP#92E	SP-210350	0299	4	F	Resolve ENs for clause 6.1A.3.2	17.1.0
2021-06	SP#92E	SP-210350	0300	3	F	Data collection within AoI for specific UEs	17.1.0
2021-06	SP#92E	SP-210350	0304	5	F	Miscellaneous correction(s)	17.1.0
2021-06	SP#92E	SP-210348	0305	3	B	Definition of Nnwdaf_MLModelInfo_Request procedure and services	17.1.0
2021-06	SP#92E	SP-210348	0306	2	B	ADRF functional description	17.1.0
2021-06	SP#92E	SP-210348	0307	-	B	Editor's note resolution for data and analytics collection via messaging framework	17.1.0
2021-06	SP#92E	SP-210573	0308	4	B	DCCF services definition	17.1.0
2021-06	SP#92E	SP-210349	0309	-	B	MFAF services definition	17.1.0
2021-06	SP#92E	SP-210349	0310	1	B	Data collection profile parameters	17.1.0
2021-06	SP#92E	SP-210349	0311	1	B	Clarify the procedure for exposing Service Experience to a MEC	17.1.0
2021-06	SP#92E	SP-210349	0315	1	B	Update the procedure for Data Collection from NWDAF	17.1.0
2021-06	SP#92E	SP-210349	0318	4	B	Update to NF Load Analytics	17.1.0
2021-06	SP#92E	SP-210349	0319	1	B	Update to time coordination across multiple NWDAF instances	17.1.0
2021-06	SP#92E	SP-210350	0320	-	C	Correlation ID for transfer of analytics subscription	17.1.0
2021-06	SP#92E	SP-210349	0322	1	B	Analytics aggregation - EN resolutions	17.1.0
2021-06	SP#92E	SP-210349	0323	-	B	Analytics aggregation - analytics metadata provisioning	17.1.0
2021-06	SP#92E	SP-210349	0324	1	B	Analytics aggregation - analytics metadata content	17.1.0
2021-06	SP#92E	SP-210349	0326	3	B	User Data congestion analytics update	17.1.0
2021-06	SP#92E	SP-210349	0329	-	B	Analytics transfer service operations	17.1.0
2021-06	SP#92E	SP-210349	0330	3	B	Extension of Naf_EventExposure for observed service experience data collection from UEs	17.1.0
2021-06	SP#92E	SP-210333	0334	1	A	Clarification on output parameters in OSE	17.1.0
2021-06	SP#92E	SP-210349	0336	1	B	Data collection from UE Application	17.1.0
2021-06	SP#92E	SP-210349	0337	1	B	Mapping UE IP address and GPSI	17.1.0
2021-06	SP#92E	SP-210349	0338	1	B	User consent to data collection and analytics	17.1.0
2021-06	SP#92E	SP-210350	0341	1	F	Adding clarifications related to the Supported Analytic Delay	17.1.0
2021-06	SP#92E	SP-210349	0342	-	B	Dispersion Analytics and DN Performance Analytics to Table 7.1-2	17.1.0
2021-06	SP#92E	SP-210349	0343	1	B	Addition of sets of NWDAF identifiers involved in analytics aggregation	17.1.0
2021-06	SP#92E	SP-210350	0348	1	F	Update to slice load analytics procedure	17.1.0
2021-06	SP#92E	SP-210349	0351	1	B	Removal of FFS Clause 6.2.2.1 on determining data sources in area of interest	17.1.0
2021-06	SP#92E	SP-210350	0352	1	F	Clarification on data storage in ADRF	17.1.0
2021-06	SP#92E	SP-210350	0353	1	F	Analytics Subscription Transfer for aggregator NWDAF	17.1.0
2021-06	SP#92E	SP-210349	0355	1	B	Clarification on the NWDAF decomposition	17.1.0
2021-06	SP#92E	SP-210349	0356	1	B	Analytics request to collect data from UE for any UE	17.1.0
2021-06	SP#92E	SP-210349	0359	-	B	Update to Contents of Analytics Exposure	17.1.0
2021-06	SP#92E	SP-210349	0360	1	B	Update to NF Load Analytics Output data	17.1.0
2021-06	SP#92E	SP-210349	0361	1	B	Update to UE Data Collection	17.1.0
2021-06	SP#92E	SP-210349	0362	1	B	ML Model Provisioning filter information	17.1.0
2021-06	SP#92E	SP-210350	0363	1	F	Clarification of Application Server address within Analytics Filter information in DN Performance Analytics	17.1.0
2021-06	SP#92E	SP-210350	0364	1	F	Clarification of Application Server address within Analytics Filter information in Service Experience Analytics	17.1.0
2021-06	SP#92E	SP-210350	0366	1	F	Correction to UE communication analytics for PDU session	17.1.0

						inactivity timer	
2021-06	SP#92E	SP-210350	0368	1	F	Dispersion analytics update	17.1.0
2021-06	SP#92E	SP-210349	0369	1	B	Processing and Processing Instructions	17.1.0
2021-06	SP#92E	SP-210350	0370	1	B	Analytics Data Repository procedures and Historical Data Handling procedure	17.1.0
2021-06	SP#92E	SP-210350	0371	-	B	Procedure for data removal from ADRF	17.1.0
2021-06	SP#92E	SP-210350	0372	-	F	Alignment with ADRF functional description and ADRF service operations	17.1.0
2021-06	SP#92E	SP-210350	0374	1	B	Procedure for Historical Data and Analytics Storage via Notifications	17.1.0
2021-09	SP#93E	SP-210921	0377	1	F	Resolving editor's notes for references to NWDAF services and cleanup for call flows	17.2.0
2021-09	SP#93E	SP-210921	0378	-	F	DCCF for data collection from applications in the UE	17.2.0
2021-09	SP#93E	SP-210921	0379	1	F	ADRF ID in Nmfaf_3daDataManagement_Configure service operation	17.2.0
2021-09	SP#93E	SP-210922	0381	1	B	KI#15 - User consent	17.2.0
2021-09	SP#93E	SP-210921	0382	1	B	Collection of input data for Analytics ID Load level information	17.2.0
2021-09	SP#93E	SP-210921	0383	1	C	Defines the Analytics Context identifiers	17.2.0
2021-09	SP#93E	SP-210921	0384	1	C	Updates to Analytics Context information	17.2.0
2021-09	SP#93E	SP-210921	0385	1	C	Updates for Analytics Context Information Transfer	17.2.0
2021-09	SP#93E	SP-210921	0386	1	F	NWDAF procedures for Analytics transfer update	17.2.0
2021-09	SP#93E	SP-210921	0387	1	B	NWDAF selection including transfer of Analytics context	17.2.0
2021-09	SP#93E	SP-210921	0388	1	C	NWDAF re-selection for Multiple NWDAF deployments - procedures -update	17.2.0
2021-09	SP#93E	SP-210921	0389	1	F	Data collection from AF support for internal group ID	17.2.0
2021-09	SP#93E	SP-210921	0390	-	F	Editorial fix in clause 5.2	17.2.0
2021-09	SP#93E	SP-210921	0393	-	C	Update to Suspicion of DDoS attack	17.2.0
2021-09	SP#93E	SP-210921	0394	1	C	Application ID - an optional input in Dispersion Analytics	17.2.0
2021-09	SP#93E	SP-210921	0395	-	F	Correction to reference descriptions for slice load level analytics	17.2.0
2021-09	SP#93E	SP-210921	0396	-	B	Removing EN on Frequency in OSE	17.2.0
2021-09	SP#93E	SP-210907	0398	1	A	Clarify the data source of UE behavioural information and expected UE behavioural parameters	17.2.0
2021-09	SP#93E	SP-210921	0400		F	Remove the FFS on how to remove the noise data by the abnormal UE list	17.2.0
2021-09	SP#93E	SP-210921	0401	1	F	Alignment of the ML Model subscription and ML Model request	17.2.0
2021-09	SP#93E	SP-210921	0404	1	F	Clarify the Analytics Filter Information of the ML Model provisioning	17.2.0
2021-09	SP#93E	SP-210921	0406	1	F	Update to analytics summary table	17.2.0
2021-09	SP#93E	SP-210922	0407	1	F	Correction for slice restrictions information	17.2.0
2021-09	SP#93E	SP-210921	0409	1	F	Correction to Annex A reference	17.2.0
2021-09	SP#93E	SP-210921	0410	1	F	Resolve EN on how the level of accuracy can be derived for analytics reports	17.2.0
2021-09	SP#93E	SP-210921	0411	1	F	Correction to NWDAF Data management service operation	17.2.0
2021-09	SP#93E	SP-210921	0412	-	F	Correction in General description of DN Performance Analytics	17.2.0
2021-09	SP#93E	SP-210921	0414	1	F	Corrections and clarifications related to analytics subscription transfer	17.2.0
2021-09	SP#93E	SP-210921	0417	1	F	Corrections related to analytics aggregation	17.2.0
2021-09	SP#93E	SP-210921	0421	1	F	Clarification on the usage of Supported Analytics Delay when the NWDAF also supports Analytics Aggregation	17.2.0
2021-09	SP#93E	SP-210922	0424	-	F	Clarification on Analytics Subscription Transfer	17.2.0
2021-09	SP#93E	SP-210922	0426	1	F	Mapping information update in UE data collection procedure	17.2.0
2021-09	SP#93E	SP-210922	0427	2	F	Miscellaneous correction for TS 23.288	17.2.0
2021-09	SP#93E	SP-210922	0428	1	F	Update description for AF registration to the NRF in TS 23.288	17.2.0
2021-09	SP#93E	SP-210922	0429	1	F	Clarifying that some data types for a specific UE collected from OAM via MDT	17.2.0
2021-09	SP#93E	SP-210922	0430	2	F	Clarify and complement the data source for data collection for NWDAF containing MTLF	17.2.0
2021-09	SP#93E	SP-210922	0431	1	F	Clarification about the Application ID in the NF profile for AF registration to the NRF	17.2.0
2021-09	SP#93E	SP-210922	0432	1	F	ML model storage alignment	17.2.0
2021-09	SP#93E	SP-210922	0433	-	F	Clarification on the NWDAF or AF triggered mapping procedure	17.2.0
2021-09	SP#93E	SP-210922	0434	1	F	Removal of EASDF	17.2.0
2021-12	SP#94E	SP-211292	0437	1	F	Add mute to DataManagement service	17.3.0
2021-12	SP#94E	SP-211292	0438	1	F	Correcting inconsistencies for analytics transfer	17.3.0
2021-12	SP#94E	SP-211292	0439	1	F	UDM-based discovery of NWDAF in Analytics Aggregation procedure	17.3.0
2021-12	SP#94E	SP-211292	0441	-	F	Alignment of NWDAF services Example Consumers with corresponding procedures	17.3.0
2021-12	SP#94E	SP-211292	0443	1	F	Clarify the OSE analytics per RAT type and/or per Frequency	17.3.0
2021-12	SP#94E	SP-211292	0444	1	F	Alignment and corrections related to accuracy, confidence, and normative wording in notes	17.3.0
2021-12	SP#94E	SP-211292	0445	1	F	Alignment, clarifications, corrections related to KI#2 and KI#11	17.3.0
2021-12	SP#94E	SP-211292	0447	1	F	Clarification for Supported Analytics Delay when reporting mode is requested	17.3.0

2021-12	SP#94E	SP-211292	0449	1	F	Clarify the Analytics target period	17.3.0
2021-12	SP#94E	SP-211292	0450	3	F	Clarify the content of ML model provisioning	17.3.0
2021-12	SP#94E	SP-211292	0451	1	F	Clarify the Slice load level analytics	17.3.0
2021-12	SP#94E	SP-211292	0453	2	F	Clarification on Per-UE Service Experience Request Procedure	17.3.0
2021-12	SP#94E	SP-211293	0455	3	F	Restriction for 5GC to provide UE IP address to untrusted AF	17.3.0
2021-12	SP#94E	SP-211292	0456	1	F	Update on Analytics context transfer and clarification on Termination Request	17.3.0
2021-12	SP#94E	SP-211292	0457	1	F	Clarifications on transfer of analytics context and analytics subscription	17.3.0
2021-12	SP#94E	SP-211292	0458	1	F	Clarifications on prepared analytics transfer	17.3.0
2021-12	SP#94E	SP-211292	0459	1	F	Clarifications on analytics aggregation	17.3.0
2021-12	SP#94E	SP-211292	0461	1	F	Clarify the NWDAF (MTLF) and NWDAF (AnLF)	17.3.0
2021-12	SP#94E	SP-211292	0463	3	F	Clarify the UE aggregated mobility analytics exposure to NF	17.3.0
2021-12	SP#94E	SP-211292	0464	-	F	Content correction of user consent	17.3.0
2021-12	SP#94E	SP-211292	0465	1	F	Clean up for UE data reporting procedure	17.3.0
2021-12	SP#94E	SP-211292	0467	3	F	Miscellaneous corrections for TS 23.288 on eNA_ph2	17.3.0
2021-12	SP#94E	SP-211292	0468	1	F	Clarification for analytics exposure via NWDAF(hosting DCCF)	17.3.0
2021-12	SP#94E	SP-211292	0469	1	F	Clarification for analytics subscription termination request	17.3.0
2021-12	SP#94E	SP-211293	0471	1	F	Correction on NWDAF reselectioin	17.3.0
2021-12	SP#94E	SP-211275	0474	1	A	Add the description of Wrong destination address	17.3.0
2021-12	SP#94E	SP-211293	0475	1	F	Clarifications for Ndccf services and Nnwdaf_DataManagement services	17.3.0
2021-12	SP#94E	SP-211293	0476	1	F	Clarify the resource usage for a network slice instance	17.3.0
2021-12	SP#94E	SP-211293	0478	1	F	Clarification on external triggers and clean up the UE mobility analytics	17.3.0
2021-12	SP#94E	SP-211293	0479	1	F	Clarifications for UE data collection	17.3.0
2021-12	SP#94E	SP-211293	0480	1	F	User consent for analytics and model training	17.3.0
2021-12	SP#94E	SP-211293	0481	1	F	Term alignment of Target of Analytics Reporting and Analytics Filter Information	17.3.0
2021-12	SP#94E	SP-211293	0482	1	F	Adding a list to enumerate NF services for enhanced procedures data collection	17.3.0
2021-12	SP#94E	SP-211293	0484	1	F	Termination request or rejection of NWDAF data managment service due to user consent not granted	17.3.0
2021-12	SP#94E	SP-211293	0486	1	F	Corrections to discovery for NWDAF containing MTLF	17.3.0
2021-12	SP#94E	SP-211293	0490	1	F	Alignment and corrections related to prepared analytics transfer	17.3.0
2021-12	SP#94E	SP-211293	0491	1	F	Clarification on interaction between timers and supported analytics Delay	17.3.0
2021-12	SP#94E	SP-211293	0492	1	F	Resolve normative wording in notes	17.3.0
2021-12	SP#94E	SP-211293	0493	1	B	DCCF-based user consent checking	17.3.0
2022-03	SP#95E	SP-220056	0425	2	F	Update of Data collection from OAM	17.4.0
2022-03	SP#95E	SP-220056	0489	2	F	Clarification on including location information for OSE analytics	17.4.0
2022-03	SP#95E	SP-220056	0494	1	F	ADRF ID in the analytics context between NWDAFs	17.4.0
2022-03	SP#95E	SP-220056	0496	-	F	Correction for the figure of DN Performance Analytics	17.4.0
2022-03	SP#95E	SP-220056	0497	1	F	Clarification on Dispersion Analytic for identification of Top-Heavy UEs in a location	17.4.0
2022-03	SP#95E	SP-220056	0499	1	F	Clarification on identifiers used as Target of Analytics Reporting	17.4.0
2022-03	SP#95E	SP-220056	0500	1	F	Correction on Analytics ID on Service Experience	17.4.0
2022-03	SP#95E	SP-220056	0504	1	F	Clarification for Analytics Aggregation without Provision of Area of Interest	17.4.0
2022-03	SP#95E	SP-220056	0505	1	F	Update for the user consent checking	17.4.0
2022-03	SP#95E	SP-220056	0506	1	F	Remove the redundant content of performance data collected from SMF	17.4.0
2022-03	SP#95E	SP-220056	0507	-	F	Remove the statistics value or expected value for load level	17.4.0
2022-03	SP#95E	SP-220056	0508	1	F	Clarification on UE related analytics	17.4.0
2022-03	SP#95E	SP-220056	0509	1	F	Correction on service operation to retreive the number of UE and number of PDU session	17.4.0