



वर्गीय आवश्यकताओं के लिए मानक

टीईसी 59080:2022

(सं:टीईसी/जीआर/एसडबल्यू/डीएससी-001/01/मार्च13 को अधिक्रमित करता है)

STANDARD FOR GENERIC REQUIREMENTS

TEC 59080:2022

(Supersedes No. TEC/GR/SW/DSC-001/01/Mar13.)

डायमीटर सिग्नलिंग कंट्रोलर

DIAMETER SIGNALING CONTROLLER



ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुरशीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI-110001, INDIA

www.tec.gov.in

© 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 02: April, 2022

Price: Free of Cost

FOREWORD

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 Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document specifies the generic requirement for the Diameter Signaling Controller (herein after referred as DSC). It shall provide Diameter protocol routing, mediation and interworking functions to manage legacy to LTE and LTE to LTE roaming seamlessly.

CONTENTS

Clause	Particulars	Page No.
	History Sheet	05
	References.....	06
	<i>Chapter 1</i>	
1.0	Introduction.....	07
2.0	Description.....	10
3.0	Functional/Operational Requirements	13
4.0	Interface Requirements.....	21
5.0	Quality Requirements	24
6.0	EMI/EMC Requirements	26
7.0	Safety Requirements.....	30
8.0	Security Requirements.....	31
	<i>Chapter 2</i>	
9.0	Information for the procurer of product.....	33
	Abbreviations	35

HISTORY SHEET

S.No.	Standard No.	Title	Remarks
1.	TEC/GR/SW/DSC-001/01/Mar13	Diameter Signaling Controller	Issue 1
2.	TEC 59080:2022	Diameter Signaling Controller	Issue 2

DRAFT

REFERENCES

RFC3588, RFC4960,RFC 4006,RFC 793,RFC 5719and RFC6733	
ISO 9001	
3GPP standards (29.805 and 29.305).	
3GPP TS 29.215 3GPP TS 29.203,TS 29.212, TS 29.213 and TS 29.214 3GPP TS 29.272 3GPP TS 29.328 and TS 29.329 3GPP TS 32.29,TS 32.251 3GPP TS 32.225 & 32.299 3GPP TS 29.228,29.229& 29.230 GSMA IR.65, IR.80 and IR.88	
CISPR 11	EN 55011
CISPR 22	EN 55022
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11

CHAPTER-1

1.0 Introduction

- 1.1 This document specifies the generic requirement for the Diameter Signaling Controller (herein after referred as DSC). It shall provide Diameter protocol routing, mediation and interworking functions to manage legacy to LTE and LTE to LTE roaming seamlessly. By avoiding the need of complex integration and customization projects, it provides a simple, reliable, and easy to deploy solution to the most challenging control plane connectivity issues.
- 1.2 Wherever, the standardized documents like ITU-T, IEEE, QA and TEC documents are referred; the latest issue and number with amendments shall be applicable.
- 1.3 The RFC documents of the IETF are subject to periodic revision. Hence where ever RFC's are mentioned in this document, the offered product shall meet either the referred RFC or its latest version. Wherever a feature of the RFC is mentioned, product shall comply with the part of the RFC specifying the feature.
- 1.4 The interpretation of the clauses of the RFC's shall be as per RFC 2119.
- 1.5 It addresses security, interoperability and scaling challenges in next-generation Long Term Evolution (LTE) and IP Multimedia Subsystem (IMS) networks. It provides critical control functions viz. congestion control, mediation and routing for Diameter transactions and sessions for subscriber authentication, authorization, mobility, and charging and quality of service (QoS). It also provides a protocol that can manage hundreds of millions of subscribers at the same time – all of whom will be accessing data, roaming from network to network, and using advanced mobile features over their devices.
- 1.6 It shall centralize signaling and Diameter routing, traffic management, and load balancing tasks to scale and grow IMS and LTE networks incrementally and cost effectively, while increasing resiliency and reliability to support subscribers' ever increasing service and broadband demands.
- 1.7 Earlier, network signaling was activated when a phone call began and ended when the two speakers hung up. Today's telecom network growth is fueled by data traffic, voice has taken back seat. These days' phones are constantly connected through the network and there is a never-ending stream of data between networks and smartphones. Diameter adds a protocol layers that

allows networks of many different types to communicate with one another. It allows 2G, 3G and 4G users to co-exist on the same network – and roam from one network to another seamlessly.

1.8 It can be deployed as an IETF Diameter Agent (relay, proxy, redirect and translation), 3GPP Diameter Routing Agent (DRA), GSMA Diameter Edge Agent (DEA) and 3GPP Interworking Function (IWF).

1.9 It shall meet the demanding requirements posed by the growing volume of signaling traffic and the complexity of connectivity and signaling in LTE and IMS networks with advanced Diameter Gateway, Diameter Load Balancer, and Diameter solutions, consolidated on a single unified platform.

1.10 A Diameter Signaling Controller has the following features

1.10.1 Simplifies the mesh of connections between the Diameter nodes and organizes the routing of packets within the core network.

1.10.2 Performs load balancing to reduce the number of network connections. Can also assure weighted load balancing of Diameter messages to various endpoints.

1.10.3 Provides network congestion control.

1.10.4 Improves interoperability between multivendor network endpoints, by creating a centralized point for Diameter signaling management.

1.10.5 Maintains session state and helps ensure that the same subscriber/session is serviced by the same network element (for example, PCRF, OSC, HSS)

1.10.6 Provides protocol translation and customization capabilities.

1.10.7 DSC enables operators to increase the resiliency and reliability necessary to support new, complex services to their customers and to scale and grow IMS, and 2G/3G/4G networks.

1.11 There are also other benefits that DSC can provide

1.11.1 Central maintenance and management point

1.11.2 Routing based on any Attribute Value Pair (AVP) content (e.g. host, realm, Q&S, location)

- 1.11.3 Routing based on external systems like Lightweight Directory Access Protocol (LDAP), or ENUM or services like Simple Object Access Protocol (SOAP)
- 1.11.4 Reduced time of change implementation
- 1.11.5 Topology hiding
- 1.11.6 All functionalities of IETF Agents: Relay, Proxy, Redirect and Translation ,3GPP Diameter Router Agent (DRA), Subscription Locator Function (SLF) and Interworking Function (IWF), GSMA Diameter Edge Agent

Figure 1 depicts, how a complicated mesh network can be converted into a simple connected network using a DSC

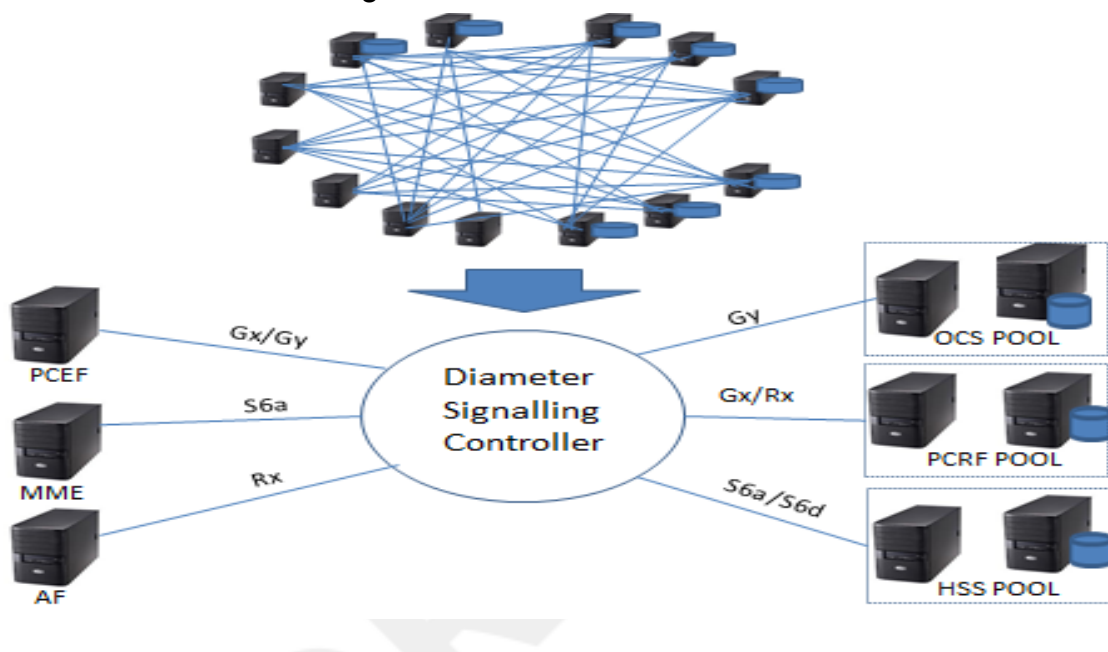


Figure -1

2.0 Description

2.1 Deployment modes:

The Diameter Signaling Controller can be deployed in different modes which would depend on the need of the service provider. Different deployment modes are as follows;

2.1.1 As part of Core network:

In this mode the Diameter Signaling Controller enables management and scaling of the internal network.

When deployed in the core network, it reduces the operational burden posed by the peer-to-peer connectivity architecture defined between the different Diameter based network elements. In core network deployment, it provides:

- i) Centralized management of Diameter signaling routing and flexibility in network configuration
- ii) Functionality for scaling up of the Diameter based servers
- iii) Functionality for overload and failover management
- iv) Mechanisms for message normalization and adaptation between Diameter variants and between Diameter and legacy protocols
- v) In core network deployment, it can serve as Proxy or Redirect routing:
- vi) In proxy mode, all Diameter transactions between two Diameter nodes are transferred through Diameter Signaling Controller.
- vii) In redirect mode, Diameter Signaling Controller participates in session establishment between two Diameter nodes, but it does not handle the Diameter transactions.

2.1.2 Sitting on the Edge:

In this mode Diameter Signaling Controller is deployed at the edge of administrative domains, e.g. PLMN/IPX/MVNO/ISP, and enables secure and interoperable roaming and single point of attachment between the partners.

It provides the security enforcement and border control functionalities between the domains. When deployed at the edge of the network, it serves as single point of attachment for roaming partners, other service providers or IPX network. In this deployment, it:

- i) hides the Diameter network topology and performs Diameter traffic steering and routing based on predefined rules and roaming policies;

- ii) Enforces Diameter security policies incoming Diameter connection and applies message normalization and adaptation.
- iii) Does message normalization and adaptation between Diameter variants and between Diameter and legacy protocols.
- iv) It serves as an IWF function defined by 3GPP standards (29.305).
- v) In edge deployment, it works as Diameter Proxy agent.

2.1.3 As Dual mode:

In this mode Diameter Signaling Controller performs both the functionalities pertaining to core as well as edge. It performs traffic steering between domains based on the supported roaming agreements. When deployed in IPX carrier/wholesale carrier/roaming hubs, it provides a secure platform to protect the network and properly route Diameter traffic at ingress and egress points.

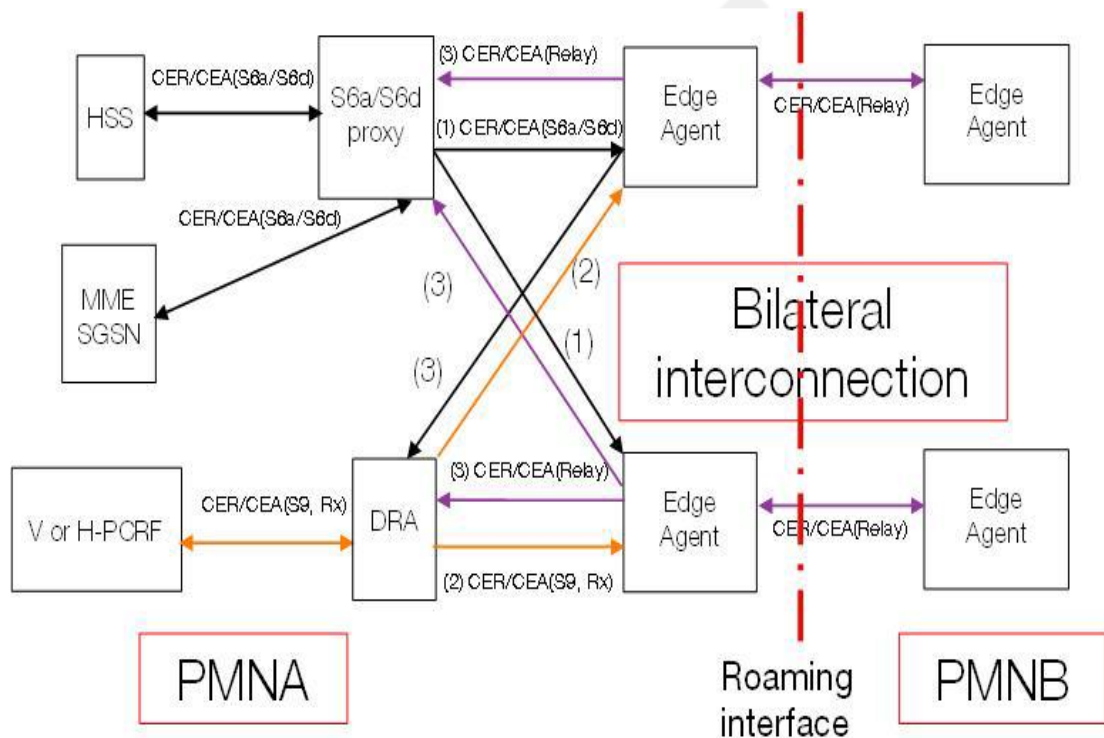


Figure 2 illustrates the case where the PMN has implemented relays at the edge and application specific proxies in the core network including a Diameter Routing Agent for Rx applications.

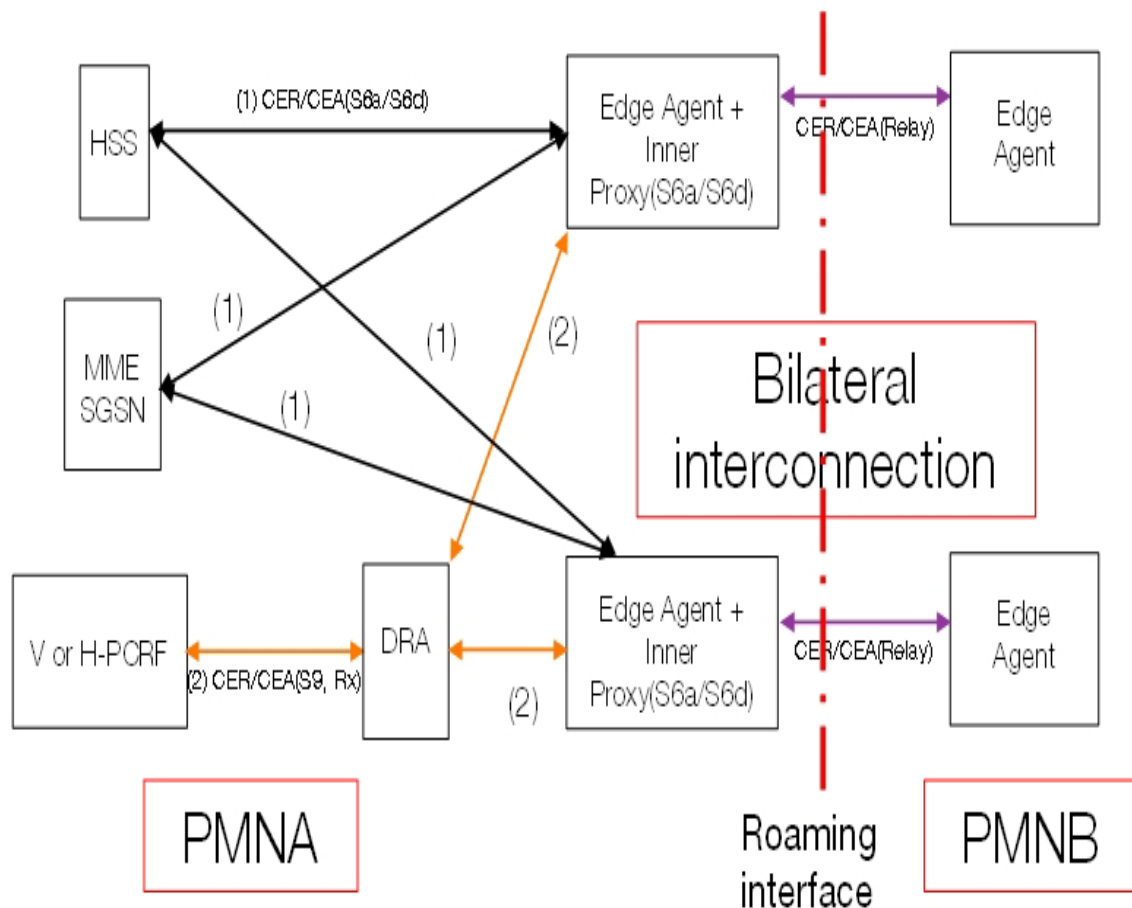


Figure 3 illustrates the case where the PMN has:

- Edge agents that are S6a/S6d proxies and relays for other applications (S9 and Rx in the current example)
- A Diameter Routing Agent to manage S9 and Rx applications in the core network

3.0 Functional/Operational Requirements

- 3.1 The DSC shall be compliant to RFC6733- Diameter Based Protocol
- 3.2 The DSC shall be compliant to RFC4960-Stream Control Transmission Protocol
- 3.3 The DSC shall be compliant to RFC 793- Transmission Control Protocol
- 3.4 The DSC shall be compliant to RFC 6733 - updated IANA considerations for Diameter Command code Allocations

3.5 Reliability, Scalability and Deployment

- 3.5.1 The DSC shall provide operations and maintenance tools and capabilities.
- 3.5.2 The DSC shall support five nines reliability level (99.999% uptime)
- 3.5.3 The DSC shall support local and geographical redundancy
- 3.5.4 The DSC must support a scalable architecture. The solution must be scalable by addition of additional Servers/blades to the architecture. The addition of scalability aspects must not impact existing network deployment
- 3.5.5 The DSC shall host multiple identities.
- 3.5.6 The DSC must support a NMS for centralized configuration mechanism for each site.
- 3.5.7 The subscriber based resolution data shall be provisioned from a centralized location and distributed to all the DSC network elements in a real-time fashion.
- 3.5.8 The subscriber provisioning Server must keep provisioning transaction logs for at least 30 days.
- 3.5.9 The ability to provide an off-board backup like provisioning logs, configuration shall be made available on fixed time interval (weekly/Monthly/Quarterly) as required by the Operator.
- 3.5.10 The DSC must support a bulk import/export utility for provisioning/configuration data
- 3.5.11 The DSC in its minimum configuration shall be rated at higher than or equal to 5,000 Diameter Transactions per Second

- 3.5.12 When configured to route requests via proxy, the DSC shall support failover on PCRF node failure and fallback on PCRF node recovery.
- 3.5.13 The DSC shall support a multi-region deployment where each region can be autonomous or shared with respect to subscriber data.
- 3.5.14 The DSC shall be deployable at the border of a network region in order to reduce number of the security associations required between PCC components.
- 3.5.15 The DSC shall be capable of being deployed collocated with a PCRF.
- 3.5.16 The DSC shall use SLF (database, or other repository) that can be collocated or remote to the DSC component.
- 3.5.17 The DSC shall support separation of internal and external network interfaces
- 3.5.18 The DSC shall support usage of VLAN to separate logical interfaces
- 3.5.19 The DSC shall support single VIP architecture for all interconnected nodes (e.g HSS, MME, PCRF, PGW). The VIP architecture shall hide internal topology of the DSC.
- 3.5.20 The VIP architecture of the DSC shall support both SCTP (including multi-homing) and TCP
- 3.5.21 The DSC shall support transparent scalability; adding new hardware shall not have impact on the external interconnected peers.

3.6 Functionality – Routing

- 3.6.1 The DSC shall support Diameter Proxy functionality and Diameter Relay and Re-direct functions (RFC 6733).
- 3.6.2 The DSC shall support mixed methods of routing: proxy and redirect.
- 3.6.3 The DSC shall be capable of routing requests from clients, e.g. AF/PCEF/BBERF to the appropriate PCRF using the Diameter Redirect and Proxy methods. The routing requirement is not limited to AF/PCEF/BBERF and PCRF.

- 3.6.4 The DSC shall support inter-PLMN Proxy Agent discovery using local routing tables.
- 3.6.5 The DRA shall support inter-PLMN Proxy Agent discovery using NAPTR, S-NAPTR, SRV and AAA DNS records.
- 3.6.6 The DSC shall support the definition of independent routing rules for each roaming agreement, definition of each routing rule shall include multiple customer configurable parameters, e.g. realm(s), PLMN-Id, Diameter Applications, etc
- 3.6.7 The DSC shall allow user to configure different roaming management/policies to be applied to each roaming agreement. Roaming policies shall include but not be limited to applications allowed to roam (S6a and/or S6d), Diameter Adaptation rules to be applied, routing rules to be applied, etc.
- 3.6.8 The DSC shall support flexible routing mechanisms; routing criteria shall be user configurable and shall include e.g. Destination Realm and/or Host; and/or Source Realm and/or Host; and/or Application-ID; and/or IMSI/MSISDN range; and /or APN.
- 3.6.9 The DSC shall be capable of resolving the PCRF/HSS or pool of PCRF/HSS for a given e.g. UE and APN.
- 3.6.10 The DSC shall support routing scenarios where the PDN-GW and/or AF are located in the home region and the UE is attached in the visited region.
- 3.6.11 The DSC solution shall support routing scenarios where the PDN-GW and/or AF are located in the visited region and the UE is attached in the visited region.
- 3.6.12 The DSC redirect host usage shall be configurable on a per-client type, e.g. AF/PCEF/BBERF.
- 3.6.13 The DSC shall handle network repartitioning without impacting active sessions, e.g. an IMSI range is split between two PCRF pools (regions).
- 3.6.14 Existing sessions shall be aged out gracefully and new sessions shall be established on the new server.

3.6.15 The DSC shall support working with SLF. The SLF shall resolve logical PCRF/HSS or pool of PCRF/HSS to e.g. UE or APN. The SLF can be collocated with DSC or located on remote server. The SLF shall implement an interface that support resolution using any configurable AVP set/range; e.g. using IMSI/MSISDN/IMPU/IMPI/NAI/UE address /.-range or APN.

3.6.16 The SLF shall support both push and pull modes of operation.

Note: It is assumed that the DSC SLF is configured through a single provisioning point and replicated such that it is accessible network-wide by all DSC in local or multi-regional deployment.

3.6.17 The DSC shall support routing decision replication and caching per IP-CAN/PCC session or other set of AVPs between all DSCs in local or multi-regional deployment.

Note: Caching expiry shall be configured based on user requirements.

3.6.18 The DSC shall support bi-directional routing, e.g. a HSS can send messages to MME out of session

3.6.19 The DSC shall be able to automatically update routing decision based on analysis of server answers or Result-Codes such as 3006, 3002 or other

3.6.20 The DSC shall be able to bind between different Diameter interfaces for dynamic routing e.g. Gx and Rx session binding based on IP_CAN sessions parameters.

3.6.21 The DSC shall support XML or SOAP protocol for provisioning purposes using session binding functionality

3.6.22 The DSC shall be able to forward duplicated Diameter messages to another peer than the destination one.

3.6.23 The DSC shall route diameter messages based on certain Diameter parameters.

It shall be possible to configure these rules based on:

- Destination-Realm (leading, trailing characters, exact match or don't care)

- Destination-Host (leading, trailing characters, exact match, don't care or presence/absence)
- Application-ID (exact match or don't care)
- Command-Code (exact match or don't care)
- Origin-Realm (leading, trailing characters, exact match or don't care)
- Origin-Host (leading, trailing characters, exact match or don't care)

3.6.24 It shall be possible to associate a set of routing rules with a connection/peer (not Origin-Host).

3.6.25 It shall be possible to associate a set of routing rules with an application-id

3.6.26 The DSC shall support at least 10,000 rules.

3.6.27 It shall be possible to create prioritized list of peers or connections for routing messages.

3.6.28 It shall be possible to deploy the DSC in a mated configuration(optional)

3.6.29 The DSC shall be able to forward transactions to its mate when its own forwarding paths towards the destination are unavailable(optional)

3.6.30 The DSC shall be able to detect faults in remote peers or transport network links to automatically re-route messages on alternate routes

3.6.31 It shall be possible to perform routing based on the following conditions

- Alternate Routing on Answer
- Alternate Routing on Timeout
- Alternate Routing on Transport Failure

3.6.32 DSC shall support following minimum indicative values.

Parameter	Low capacity	Medium Capacity	High Capacity
TPS	5000#	20000	50000
Peers	500	2000	5000
Connections	1000	4000	10000

Signalling Latency	Not More than 50ms for core routing and 100ms for Database /Stateful Application
-----------------------	---

Here, for indicative purpose, one Transaction refers to two messages i.e. (Request/Response) in back to Back Mode between Diameter Client and Server.

3.7 **Functionality – Message manipulation**

- 3.7.1 The DSC shall advertise support of the Diameter Gx, Gxc and Rx, S6a, S6d, applications.
- 3.7.2 The DSC shall support Diameter adaptation/manipulation including, but not limited to, user configurable patterns/templates and user configurable action to be applied when positive pattern/template matching occurs (reject message, modify AVP, remove AVP, etc)
- 3.7.3 The DSC shall support user configurable usage/mapping of error codes.
- 3.7.4 The DSC shall provide trouble-shooting tools which shall include both historic data as well as real-time captures/traces capabilities.
- 3.7.5 The DSC shall support storing accounting records, data captured for each individual record shall be user configurable.
- 3.7.6 The DSC shall provide means to retrieve accounting records from external servers, both push and pull shall be supported The DSC shall support defining custom dictionary for AVP/ vendor id/application id.

3.8 **Functionality – Load Balancing**

- 3.8.1 The DSC shall provide congestion control methods, congestion thresholds shall be user configurable. Actions to be taken when thresholds are met shall also be user configurable.
- 3.8.2 The DSC shall support load balancing mechanisms.

3.8.3 When configured to route requests via proxy, the DSC shall be capable of load-balancing requests across a pool of Diameter Servers, e.g. a pool of PCRF nodes which make up a single logical PCRF.

3.8.4 The DSC load balancing functionality shall support the following methods

- a. Weighted Round Robin
- b. Round Robin
- c. Weighted least loaded
- d. Least loaded
- e. Hashed (based on set of AVP)
- f. Stickiness based on SLF selection

3.8.5 The solution shall be able to support OCS directive for session failover and apply them accordingly

3.8.6 The DSC solution shall provide methods and mechanisms to perform stateless and stateful load balancing/sharing

3.9 Functionality – Visibility and tracing

3.9.1 The DSC shall support real-time Diameter messages tracing based on certain criteria such as User-IMSI, Session-Id or any other AVP set or Client Peer.

3.9.2 The DSC shall be able to provide detailed statistics on Diameter traffic such as: RTT, TPS, Errors and other.

3.9.3 The statistics for Diameter traffic shall be available for external process retrieval.

3.10 Functionality – Overload and Capacity management

3.10.1 The DSC shall support self-overload protection.

3.10.2 The DSC shall allow enforcing message control rate to its interconnected peers. The message control rate shall be configurable per peer

3.10.3 The DSC shall provide clear notification when overload or message limit is activated

3.11 Functionality – Message Copy

3.11.1 The DSC shall support Message Copy to route Diameter request messages to external Diameter Application Server

3.11.2 DSC shall support flexible mechanisms to trigger the Message Copy function including:

- Trigger on Request message content
- Trigger by DSC Application

3.12 Functionality – Back up & Restore

3.12.1 Backup mechanism shall exist to take backup for

- a. System software backup
- b. Alarm log and internal error log backup
- c. Transaction logs backup
- d. System configuration backup
- e. Provision Data backup
- f. Charging data backup (if applicable)
- g. Both Automatic & Manual backup options shall be supported.
- h. It shall be possible to transfer the backup to external standard device.
- i. It shall be possible to take back-up for at least fifteen days of operation.
- j. It shall be possible to load back-up data, to recover the services within one hour and full normalcy of the system within eight hours.

4.0 Interface Requirements

4.1 Interfaces:

- 4.1.1 The DSC shall support Diameter to SS7/MAP interworking according to 29.305 Release 11
- 4.1.2 The DSC shall support Diameter-RADIUS interworking
- 4.1.3 The DSC shall support interworking with LDAP (Optional).
- 4.1.4 The DSC shall support S9 interface as per 3GPP TS 29.215
- 4.1.5 The DSC shall support Gx, Gxa/Gxc,Rx and Sd interfaces as per 3GPP TS 29.203,3GPP TS 29.212, TS 29.213 and TS 29.214
- 4.1.6 The DSC shall support Gy, Gz (Offline charging) interfaces as defined in TS 32.29, TS 32.251 & RFC 4006
- 4.1.7 The DSC shall support Cx interface as defined in TS 29.228 & TS29.229
- 4.1.8 The DSC shall support Rf/Ro interfaces as defined in RFC 4006, TS 32.225 & 32.299
- 4.1.9 The DSC shall support S6a & S6d interface as per 3GPP TS 29.272
- 4.1.10 The DSC shall support Sh interface as per 3GPP TS 29.328 and TS 29.329
- 4.1.11 The DSC shall support LTE roaming functionality as per GSMA IR.80 and IR.88
- 4.1.12 Depending upon the integration the DSC shall be able to support any vendor specific Attribute value pairs (AVP)

4.2 Peer Connectivity

To inter-op with other Diameter peers (Minimum 1000 Peers and 2000 connections) the DSC shall support flexible Connectivity Exchange mechanisms like

- 4.2.1 Support any Application-ID during the Capabilities exchange
- 4.2.2 Authenticate for minimum set of mandatory Application-IDs
- 4.2.3 Support more than one Vendor Specific Application-ID
- 4.2.4 Support multiple connections to a peer
- 4.2.5 Support configurable error-treatment options on a per connection/peer basis

- 4.3 **IP Addressing**(DSC shall not violate the implementation of IPv6 as per the mandate of NDCP-2018 and instruction issued by DoT HQ time to time.)
- 4.3.1 The DSC shall support both IPv6 as per RFC 8200/Dual stack as per RFC 4213 for external communication to other nodes.
 - 4.3.2 The DSC shall be capable of connecting to others peers with either of IPv4 or IPv6
 - 4.3.3 The local Processing Blade on the DSC shall be capable of supporting IPv6 as per RFC 8200/Dual stack as per RFC 4213 addressing (Applicable for purposely built hardware or physical entity)
 - 4.3.4 The DSC shall be capable of routing Diameter Requests & Answers between IPv4 & IPv6 peers
 - 4.3.5 The DSC shall have the option to configure FQDN in lieu of the Peer's IP address
 - 4.3.6 The DSC solution shall support a single point of connection (IP Front End) for all clients.
- 4.4 **Transport**
- 4.4.1 The DSC shall support both TCP & SCTP as transport protocol of choice to carry the Diameter messages
 - 4.4.2 Both TCP & SCTP shall be supported to the same Node simultaneously. Moreover, DSC shall be able to support TCP-SCTP Interworking function over different versions of IP protocol i.e IPv4 (TCP) <-> IPv6 (UDP) or vice versa.
 - 4.4.3 The DSC Shall be able to select signaling transport protocol (TCP or SCTP) for each far endpoint independently over IPv4 and IPv6, and the transport protocol to be used for transmitting the message to reach the destination shall also be configurable, TCP or SCTP
 - 4.4.4 The DSC shall be capable of routing Diameter Requests & Answers between TCP & SCTP based peers
 - 4.4.5 SCTP Multi-Homing shall be supported when connecting to other SCTP based peers.
 - 4.4.6 The DSC shall support multiple inbound & outbound SCTP streams in each SCTP association

- 4.4.7 Appropriate alarms when the SCTP connection towards a peer fails
- 4.5 **Physical Interfaces:**
 - 4.5.1 DSC shall support 1GE/10GE Electrical/Optical Interfaces for physical connectivity to other interconnected network elements with different options of SFP's including Electrical/ Optical (Single Mode/ Multimode). (Applicable for purposely built hardware or physical entity)
 - 4.5.2 DSC shall support for sharing one physical network for OAM, Control and Signaling Traffic. (Applicable for purposely built hardware or physical entity)
 - 4.5.3 DSC shall also support a separate physical network for Signaling, OAM & Control Traffic. (Applicable for purposely built hardware or physical entity)
 - 4.5.4 DSC shall provide logical separation of OAM, Control & Internal traffic via VLANs
 - 4.5.5 DSC shall support a separate physical network for signaling traffic. (Applicable for purposely built hardware or physical entity)
 - 4.5.6 DSC solution shall smoothly integrate with Operator L2 domain. (Applicable for purposely built hardware or physical entity)
 - 4.5.7 DSC solution shall allow Operator Routers/Firewalls to define the L2 boundaries. (Applicable for purposely built hardware or physical entity)

5.0 Quality Requirements

5.1 Qualitative Requirements (QR): The system shall meet the following qualitative requirements:

5.2 The equipment shall be manufactured in accordance with international standards ISO 9001 for which the manufacturer shall be duly accredited for the latest issue. A quality plan describing the quality assurance system followed by the manufacturer shall be required to be submitted. (Applicable for purposely built hardware or physical entity)

5.3 The MTBF (Mean time Between Failure) and MTTR (Mean Time to Restore) predicted and observed values shall be furnished along with calculations by the manufacturer. (Applicable for purposely built hardware or physical entity)

5.4 Reliability

5.4.1 The entire DSC solution must not have a single point of failure. Failure of a single module shall not result in a disruption of service. All critical components such as power supply, fans, management/ control modules shall be redundant.

5.4.2 The DSC solution must support at least 99.999% availability

5.4.3 The DSC solution shall be a standalone system (optional)

5.4.4 The DSC solution must support automatic failover

5.4.5 There shall be a 1:1 system backup redundancy for data

5.4.6 Logs, tracing and other OA&M activities must not impact the performance of the DSC

5.4.7 The system application design shall be modular in nature and shall have a distributed architecture

5.4.8 Removal or addition of any module shall not allow disruption of service to other modules

5.4.9 The DSC system shall be able to add new feature sets without service disruptions of affecting basic functionality

5.4.10 Describe procedures for reporting end-user customer complaints, including support availability, methods of engagement, and expected turn-around times

5.4.11 Supplier shall provide details of its warranty policies and procedures including, but not limited to a clear statement of the duration and conditions of warranties, and the warranties of Supplier's suppliers

5.5 QoS and Congestion Control

- 5.5.1 The DSC shall support prioritizing certain Requests over others
- 5.5.2 The DSC shall support limiting the number of messages that can be sent by a client (ex: MME, PGW, etc) and shedding any excess load
- 5.5.3 The DSC shall support shedding excess load when the DSC enters congestion during periods of heavy load
- 5.5.4 The DSC shall support shedding excess load when Diameter servers (HSS, OCS, PCRF, etc) experience congestion or when the total traffic arriving at the DSC from the various clients exceeds the capacity of these servers.
- 5.5.5 The DSC shall use message priority as a mechanism when shedding excess load due to ingress, egress or DSC congestion

DRAFT

6.0 EMI/EMC Requirements (Applicable for hardware (Standalone) based DSC

6.1 These requirements are applicable for purposely built hardware or a physical entity only. The equipment shall conform to the following EMC requirements for **Class A**:

General Electromagnetic Compatibility (EMC) Requirements: - The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from an accredited test agency.

a) Conducted and radiated emission (applicable to telecom equipment):

Name of EMC Standard: "CISPR 22 (2008) - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits: -

- (i) To comply with class A of CISPR 22 (2008) or CISPR 32(2015)
- (ii) The values of limits shall be as per TEC Standard No. **TEC 11016:2016**.
- (iii) For Radiated Emission tests, limits below 1 GHz shall be as per Table 4 (a) or 5 (a) for measuring distance of 10m **OR** Table 4 (a1) or 5 (a1) for measuring distance of 3m.

b) Immunity to Electrostatic discharge:

Name of EMC Standard: IEC 61000-4-2 (2008) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits: -

- i. Contact discharge level 2 { ± 4 kV} or higher voltage;
- ii. Air discharge level 3 { ± 8 kV} or higher voltage;

c) Immunity to radiated RF:

Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement Techniques-Radiated RF Electromagnetic Field Immunity test"

Limits: -

For Telecom Terminal Equipment without Voice interface (s)

Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz

and 1.4 GHz to 6.0 GHz.

d) Immunity to fast transients (burst):

Name of EMC Standard: IEC 61000- 4- 4 (2012) "Testing and measurement techniques of electrical fast transient's/burst immunity test"

Limits: -

Test Level 2 i.e. a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal / control / data / telecom lines;

e) Immunity to surges:

Name of EMC Standard: IEC 61000-4-5 (2014) "Testing & Measurement techniques for Surge immunity test"

Limits: -

i. For mains power input ports:

(a) 2 kV peak open circuit voltage for line to ground coupling

(b) 1 kV peak open circuit voltage for line to line coupling

ii. For telecom ports:

(a) 2 kV for common mode.

Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. **TEC 11016:2016**.

Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. **TEC 11016:2016**.

It may be seen that for telecom ports, surge requirement of 2 KV for L-G coupling (common mode) only has been prescribed.

f) Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: IEC 61000-4-6 (2013) "Testing & measurement Techniques-Immunity to conducted disturbances induced by radio-frequency fields"

Limits: -

Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: IEC 61000-4-11 (2004) “Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests”

Limits: -

- i. a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e. 70 % supply voltage for 500ms)
- ii. a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms)
- iii. a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.
- iv. a voltage interruption corresponding to a reduction of supply voltage of >95% for 10ms.

h) Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any):

Name of EMC Standard: IEC 61000-4-29 (2000): Electromagnetic compatibility (EMC)-PART 4-29: Testing & measurement techniques- voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests.

Limits: -

- i. voltage Interruption with 0% of supply for 10ms. Applicable Performance Criterion shall be B.
- ii. voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criterion shall be C.
- iii. voltage dip corresponding to 40% & 70% of supply for 10ms, 30ms. Applicable Performance Criterion shall be B.

Note 1: Classification of the equipment:

Class B: Class B is a category of apparatus which satisfies the class B disturbance limits. Class B is intended primarily for use in the domestic environment and may include:

- Equipment with no fixed place of use; for example, portable equipment powered by built in batteries;

- Telecommunication terminal equipment powered by the telecommunication networks
- Personal computers and auxiliary connected equipment.

Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected.

Note 2: The test agency for EMC tests shall be an ISO 17025 accredited agency and details of accreditation shall be submitted.

Note 3: For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. **TEC 11016:2016** and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (h) and TEC Standard No. **TEC 11016:2016**. The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	Euro Norm
CISPR 22	EN 55022
CISPR 32	EN 55032
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11
IEC 61000-4-29	EN 61000-4-29

The manufacturer / supplier shall submit a test certificate and test report for EMI/EMC compliance from test agency. The test agency for EMI/EMC tests shall be an ISO 17025 accredited agency and details of accreditation shall be submitted.

- 7.0 Safety Requirements (Applicable for hardware (Standalone) based DSC**
- 7.1 These requirements are applicable for purposely built hardware or a physical entity only. The equipment shall conform to IS 13252 part 1:2010- “Information Technology Equipment – Safety- Part 1: General Requirements” [equivalent to IEC 60950-1 {2005} “Information Technology Equipment –Safety- Part 1: General Requirements” or IEC 62368-1 “Audio/video, information and communication technology equipment - Part 1: Safety requirements”.
- 7.2 A test certificate and test report shall be furnished from an accredited test agency.
- 7.3 The test agency for safety requirements tests shall be an ISO 17025 accredited agency and details of accreditation shall be submitted.

DRAFT

8.0 Security Requirements

- 8.1 The DSC shall support L3/L4 access control methods
- 8.2 The DSC shall support L5 access control methods, e.g.: accept all Diameter clients without them being provisioned in the DSC.
- 8.3 The DSC shall support IPsec/IKE and TLS/DTLS for Diameter connections
- 8.4 The DSC shall be able to support features to prevent exposure of internal Diameter topology request when sending a request to an external network.
- 8.5 The DSC shall support message screening and message normalization.
- 8.6 The DSC shall be able to terminate request by answering with predefined answer or discard the request based on any AVP or any other condition e.g peer, realm.
- 8.7 The DSC shall support TLS
- 8.8 Conforming to TEC 61010:2017 and GR No. TEC 61020:2017, the system in association with Soft switches and monitoring equipment shall not pose any problem in interception and monitoring of all types of communications (voice, data, message contents of all types and FAX) for terminating, originating and transit types of calls for complete duration.

8.9 Unauthorized Access

- 8.9.1 Suitable safeguards shall be provided in the man-machine communication programs to debar unauthorised persons from making any changes in the memory contents or office data. Access to system operations shall be controlled through multi-level password and authentication checks.
- 8.9.2 The man-machine communication programs shall have the facility of restricting the use of certain commands or procedures to certain passwords and terminals
- 8.9.3 Access to system operations shall be controlled through multi-level password and authentication checks.

8.10 Monitoring

- 8.10.1 The system shall pose no limitation in interception and monitoring any signalling link from monitoring positions
- 8.10.2 Adequate security mechanisms at different levels shall be provided in the STP so as to prevent unauthorized access or interference to services, calls, protocols and data.
- 8.10.3 In case of IP connectivity with STP, the system shall have facility to prevent Denial of Service (DOS) attacks. It shall be able to interact with various elements based on known IP address (source and destination), port number (source and destination) and Interface Identity (Applicable in case IP interface is supported)
- 8.11 The applicant/manufacture shall submit a certificate from any international agency/ labs of the standards e.g. Common Criteria Labs in case of ISO/IEC 15408 standards until 31st March 2013. From 1st April 2013 a certificate from authorized and certified agencies/labs in India shall be submitted or as per any latest instruction issued by DOT in this regard shall be applicable.

CHAPTER-2

9.0 Information for the procurer of product (Desirable Requirements)

9.1 Operations & Maintenance

- 9.1.1 The DSC OAM shall require user id and password for GUI access
- 9.1.2 The solution will provide a web based or MML based GUI that will permit multiplier users to access it simultaneously to extract performance statistics. GUI shall include (but not necessarily be limited to) a thin web client that is not a java application
- 9.1.3 The solution shall have the capability to export performance statistics to an external system
- 9.1.4 The DSC solution shall have the capability to track and monitor active subscribers over a period of time. The time periods shall be at minimum per hour, per day. The data required shall be at a minimum session per sub and length on a session,
- 9.1.5 The DSC solution shall provide Measurement Reports. This must include all possible traffic information on the DSCs and other relevant metrics.
- 9.1.6 The DSC Solution shall have the capability of producing SNMP trap alarms and forward to a SNMP manager.
- 9.1.7 The DSC solution must have the ability to log all the events, alarms, and failures
- 9.1.8 The DSC solution will provide the following system health statistics: % memory usage average and peak; % cpu usage average and peak; disk usage
- 9.1.9 The DSC solution shall provide capability for software upgrade and back out. Procedures and MOP documents shall be provided for operational staffs to perform software upgrade and back out.
- 9.1.10 Complete vendor documentation for the process of adding a DSC node(s) to the production environment must be provided.
- 9.1.11 Measurement Reports must be provided. This must include traffic information on the DSCs and other relevant metrics. The fields in the reports must be stated clearly in a separate document.

- 9.1.12 The DSC Solution measurement interval must be configurable. The DSC shall have the ability to either push or have the measurement reports pulled by external network element.
- 9.1.13 Describe the kind of visibility or access to support tools that this solution provides
- 9.1.14 The DSC solution must support tracing of sessions. The decision must be based on parameters like the originating peer, destination peer and subscriber information

9.2 HARDWARE REQUIREMENTS (if required)

- 9.2.1 The proposed solution shall operate between –40 to –57.5 volts DC measured at the NE unit input power lugs for each individual power source feed.
- 9.2.2 The DSC solution shall accept dual, independent –48 VDC power sources
- 9.2.3 The DSC solution shall be powered by a –48 volt (nominal) DC power source
- 9.2.4 In the event that one of the power sources is unavailable, the equipment shall continue to operate from the remaining power source without manual intervention and without interruption of service or functionality (including all LED's, alarms, and indications).

ABBREVIATIONS

AF	Address Family
AVP	Attribute Value Pair
DNS	Domain Name Server
DRA	Diameter Routing Agent
ENUM	E.164 Number Mapping
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GRX	GPRS Roaming Exchange
GSM	Global System for Mobile Communications
GSMA	GSM Association
GW	Gateway
H/W	Hardware
hPCRF	Home PCRF
HPMN	Home PLMN
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
IP-CAN	IP Connectivity Access Network
IPSEC	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	IP Exchange
KPI	Key Performance Indicator
L2, L3, etc	Layer 2, Layer 3, etc.
LTE	Long Term Evolution
MAP	Mobile Application Protocol
MME	Mobility Management Entity
MPS	Messages Per Second
MSISDN	Mobile Subscriber ISDN Number
NAPTR	Name Authority Pointer
NMS	Network Management System.
OAM	Operation, Administration, and Maintenance

OCS	Online Changing System
OS	Operating Systems
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rule Function
PDN	Packet Data Network
P-GW	PDN Gateway
PLMN	Public Land Mobile Network
PMN	Public Mobile Network
RADIUS	Remote Authentication Dial In User Service
SCP	Secure Copy
SCTP	Stream Control Transmission Protocol
SFTP	Secure File Transfer Protocol
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SLF	Subscriber Location Function
SRV	Service DNS record
TCP	Transmission Control Protocol
TPS	Transactions Per Second
UE	User Equipment
vPCRF	Visited PCRF
VPMN	Visited PLMN

===== End of the document =====