Question(s):	16/13	**Meeting:**	Seoul, 16-20 December 2019
Study Group:	13	**Working Party:**	WP3
Source:	India		
Title:	Proposed modifications to the draft Recommendation ITU-T Y.OBF_trust: "Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems"		
Purpose:	Proposal		
Contact:	Abhay Shanker Verma TEC India	Tel: + 91 9868138506 E-mail: as.verma@gov.in	
Contact:	Ranjana Sivaram TEC India	Tel: +919868136990 E-mail: ranjana.sivaram@gov.in	
Contact:	Sharad Arora Sensorise Digital Services Pvt Ltd India	Tel: +91 9212109999 E-mail: sharad.arora@sensorise.net	

Keywords:	Open bootstrap framework; Symmetric keys; Y.OBF_trust
Abstract:	This document proposes the content for section 10.3.4 "Changing of Authentication Provider Flow (Symmetric keys)" to draft Recommendation ITU-T Y.OBF_trust.

This contribution proposes that the text in Annexure-I may be added to Section 10.3.4 "Changing of Authentication Provider Flow (Symmetric keys)" in the draft Recommendation ITU-T Y.OBF_trust: "Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems".

Base text is the output document in TD325/WP3 (Geneva, 14 -25 October 2019)

———————————————

Annexure-I

Changing of Authentication Provider Flow (Symmetric keys):

The User of the service has to approach the new M2M Service Provider / Mobile Operator for enabling the use of the Authentication Services.

1. The Steps for such a transfer are described below: User requests new Authentication Services Provider for its services

2. The new Authentication Service Provider requests existing Authentication Service Provider for User's Shared Keys

3. The new Authentication Services Provider uses the old key to update the Secure Element with a new key following the Custodian Know-Your-Customer norms applicable to that context

4. The new Authentication Services Provider informs the User and the old Authentication Services provider of the successful confirmation of the transfer to the new Authentication Services Provider

5. Upon successful confirmation of the transfer the new Authentication Services Provider informs the Application Services Providers about the change in the OBF_Token for a User

6. The Application Service Provider uses the new OBF_Token along with embedded connectivity identity to verify the User

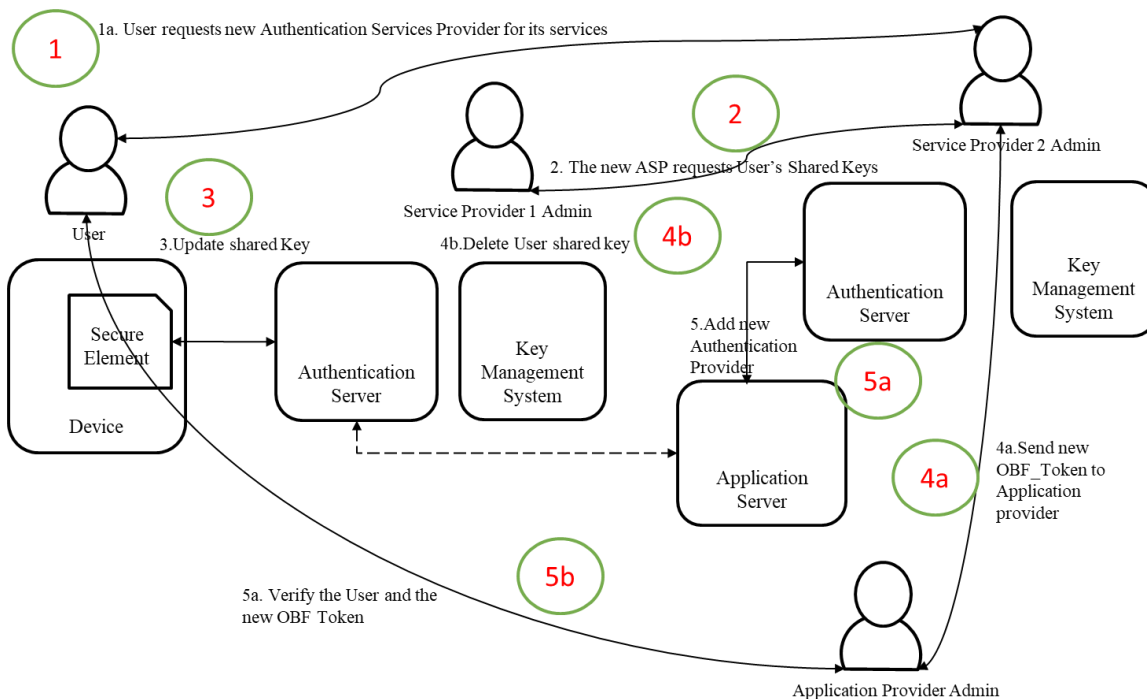The Process is described in the flow diagram below:

Figure 6: Change Authentication Service Provider (Symmetric Keys)

(Note to Rapporteur:

A new definition has to be added for OBF_Token which is work in progress.)