INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

Q16-13-May20-C118R1

Study Group 13

English only

Question(s): 16/13 e-Meeting, 18 May 2020

CONTRIBUTION

Source: Telecom Engineering Centre (TEC), Ministry of Communications, India

Title: Draft Recommendation ITU-T Y.OBF_Trust: "Open Bootstrap Framework enabling trusted devices, applications and services for distributed diverse ecosystem".

Purpose: Proposal

Contact:	Abhay Shanker Verma Telecom Engineering Centre (TEC) India	Tel: + 91 9868138506 E-mail: as.verma@gov.in
Contact:	Ranjana Sivaram Telecom Engineering Centre (TEC) India	Tel: +91 9868136990 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: Bootstrapping; IoT Service Provider; OBF; OBF Proxy; OBF_Token; Open Bootstrap Framework; Trust Framework

Abstract: This document proposes modifications in section 6 of the draft Recommendation ITU-T Y.OBF_Trust (TD416-WP3) for discussion at interim e-meeting of Q16/13.

1. Introduction

In the Editor's Note below Figure 1 in Section 6 in the output document (**TD416-WP3**) of e-meeting dated 27 April 2020, it is expected that the *overall concept of OBF to be described in more detail; OBF Architecture and Reference Model to be clearly explained; main idea of recommendation needs to be explained; and individual items need further description.* Further, it was also expected that the *diagram showing Trust Framework using OBF Reference Model may be revised with detailed explanation for more clarity.* In order to address these observations and for improved readability and more clarity, this contribution proposes to carry out modification in section 6 of the draft Recommendation ITU-T Y.OBF_Trust (**TD416-WP3**).

2. Proposal

It is proposed to modify section 6 of the draft Recommendation ITU-T Y.OBF_Trust (**TD416-WP3**) The proposed modifications are in track change mode in **Annexure-I**.

3. Reference

[1] T17-SG13-200720-TD-WP3-0416!!MSW-E: Base Document for this contribution.

_____

Annexure-I

6 Overview of the Open Bootstrap Framework

6.1 OBF Concept Model

With advancement of communication technologies and embedded electronics, a large number of new applications are likely to connect millions of users with many service providers across geographical boundaries. These diverse and distributed users and service providers will need to borrow the required trust from existing trust relationships, as it may not be possible to develop individual one to one trust relationships between the users and the millions of new age service providers. For example, Play Store and App Store provide a trust framework for the buyer of a mobile device, who is able to use applications from the Play Store or App Store as these become proxy in the relationship between the user and the application provider. This is an example of a trust framework.

This recommendation introduces a trust framework in which an ASP, hitherto unknown to the user of a connected device, can provide its applications and services by using the trust relationship between the user and the Network & IoT Service Provider. The OBF concept addresses the critical need for an inter-operable, network technology agnostic framework for sharing of trust between the Network & IoT Service Provider, ASP and the User by bootstrapping of connected devices, authentication of users and authorization of applications based on the trust provided by the Network & IoT Service Provider.

The Users and their Connected Devices are authenticated based on the bootstrapping provided by the Network & IoT Service Provider that provides the network layer security and access control. Application Service Providers use the Network layer authentication with an added layer of Authorization such as to secure the use of specific Applications to specific Users / Connected Devices. Applications so offered to the Users are referred to as Trusted Services.

The actors and their interactions are shown in the OBF concept model below.

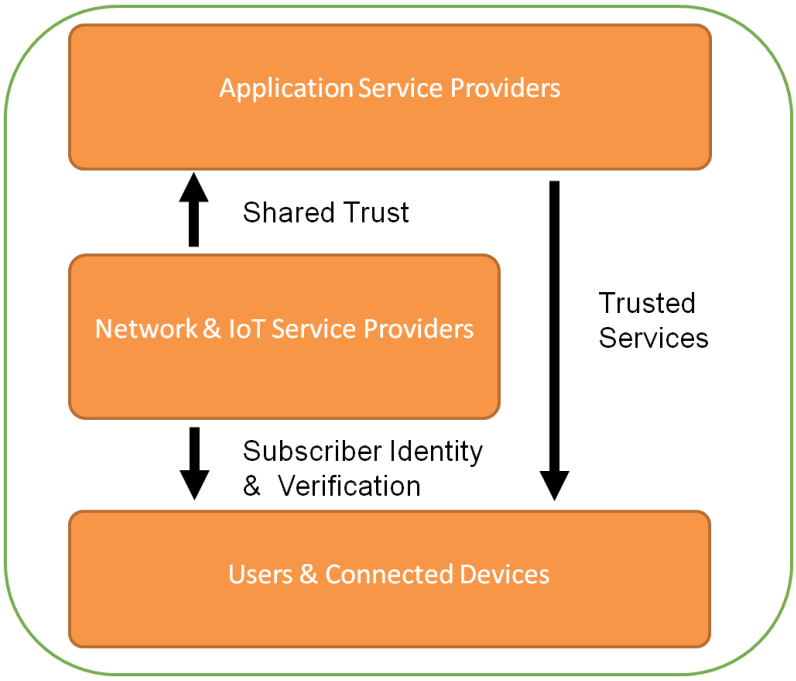

Figure 1: OBF Concept Model

6.2 OBF Service Model

From time immemorial, the Network Operator has played the role of providing connectivity to the premises of subscribers, undertaking the subscriber verification and then allowing the connectivity to be used for a diverse set of services.

In the same manner as above, where a user is able to use a diversity of services on the connectivity provided by a Network Operator, the concept of OBF extends the trust created by the subscriber verification undertaken by the Network Operator to many other Applications and Services provided by ASPs.

The trust framework of the OBF has the following key actors:

1. Network & IoT Service Provider: The Network Operator that provides the connectivity services, undertakes the physical verification of the Subscriber and shares that trust with ASPs and Users by the mechanism of the OBF. This reuse of trust, involves on the one hand, issuance and use of pre-shared keys hosted on the Secure Element, and on the other, the issuance and use of secure tokens to the ASPs.
2. Applications & Service Providers: The ASP is an entity that has developed applications for providing Trusted Services that benefit Users, and has an expectation of a minimum level of authentication and authorization for the use of the ASP's application and services by the User. However, the ASP does not have a direct relationship, unlike the one between the Network Operator and the Subscribers. The mechanisms of the OBF provide for a Subscriber of the Network Operator to become an authenticated User of the ASP. The ASP uses the secure token for establishing this trust relationship.
3. Users: The Subscribers of the Network Operator benefit from the mechanisms of the OBF, reusing the authentication and authorization for availing the Trusted Services provided by the ASP.

The OBF service model provides for the following OBF services:

1. Bootstrapping of Connected Devices to the OBF

The bootstrapping process of the OBF provides the mechanism for the existing security capabilities of the secure element provided in the Connected Devices to be put at the disposal of the OBF Client for enabling trustful identity and authentication of users and applications.

The OBF uses the unique identity and security capabilities of the tamper resilient secure element as the root of trust.

At the completion of the bootstrapping process, a Connected Device is registered to the trust framework of the OBF.

2. Authentication of the Users and Applications

The OBF Authentication Services provide mechanisms for the bootstrapped Connected Devices to be identified by the applications and for the user interactions to be secured using agreed security algorithms.

3. Authorization of ASP Services for Authenticated Users

The OBF Authorization Services provide mechanisms for the application clients and applications to interact with each other with end to end security enablement using key material and security algorithms provided by the Authentication services of the OBF.

OBF interactions result in the conversion of a verified Subscriber of a Network into an Authenticated User of the ASP, allowing Service Access to be controlled effectively by the ASP. The reference service model for the OBF is depicted in Figure 2 below:

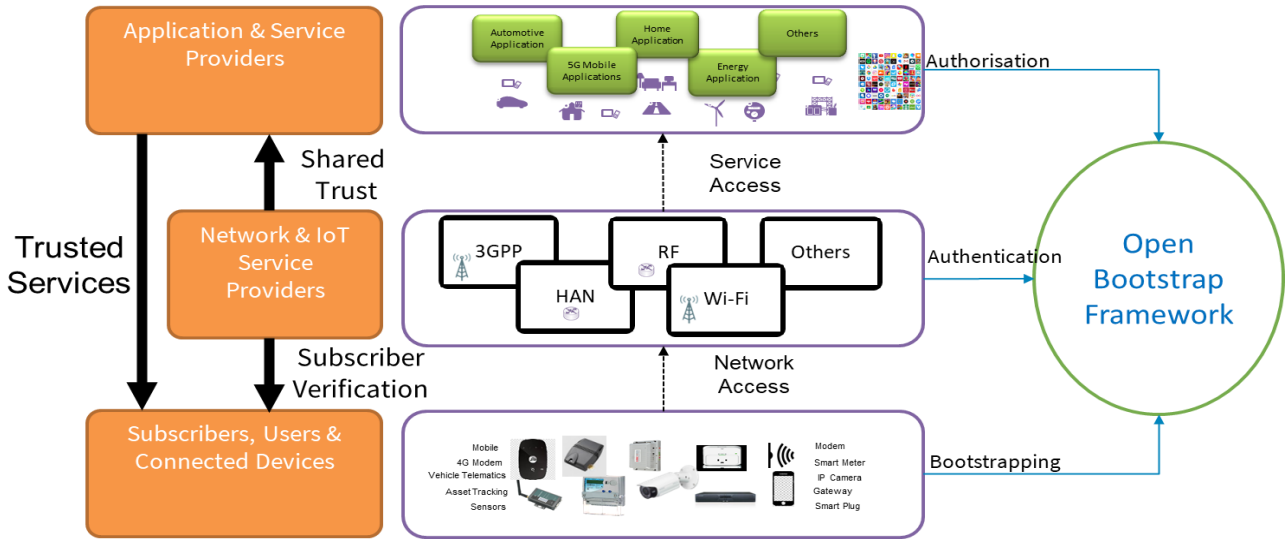

Figure 2: OBF Reference Service Model

When deployed in practice, the OBF Service Model will likely be augmented with a regulatory guideline, a collection of contracts, a defined form of collaboration, a system of enforcement mechanisms etc. such as for the actors to work together in an organized manner.

6.3 OBF Working Model

The OBF Working Model provides an interoperable, implementation-independent and scalable approach for multi-party interactions where various connected devices using a variety of network technologies are able to access applications and services securely through the OBF. The OBF utilizes the identification and authentication carried out for and by underlying technology layers, and extends it towards the ASPs for the provision of trusted services.

NOTE: The interaction of OBF with diverse network technologies, shall require an implementation specific proxy function for the underlying network technology layer. The specification of the proxy function is out of the scope of this recommendation.

The OBF working model with multiple networks is shown in Figure 3

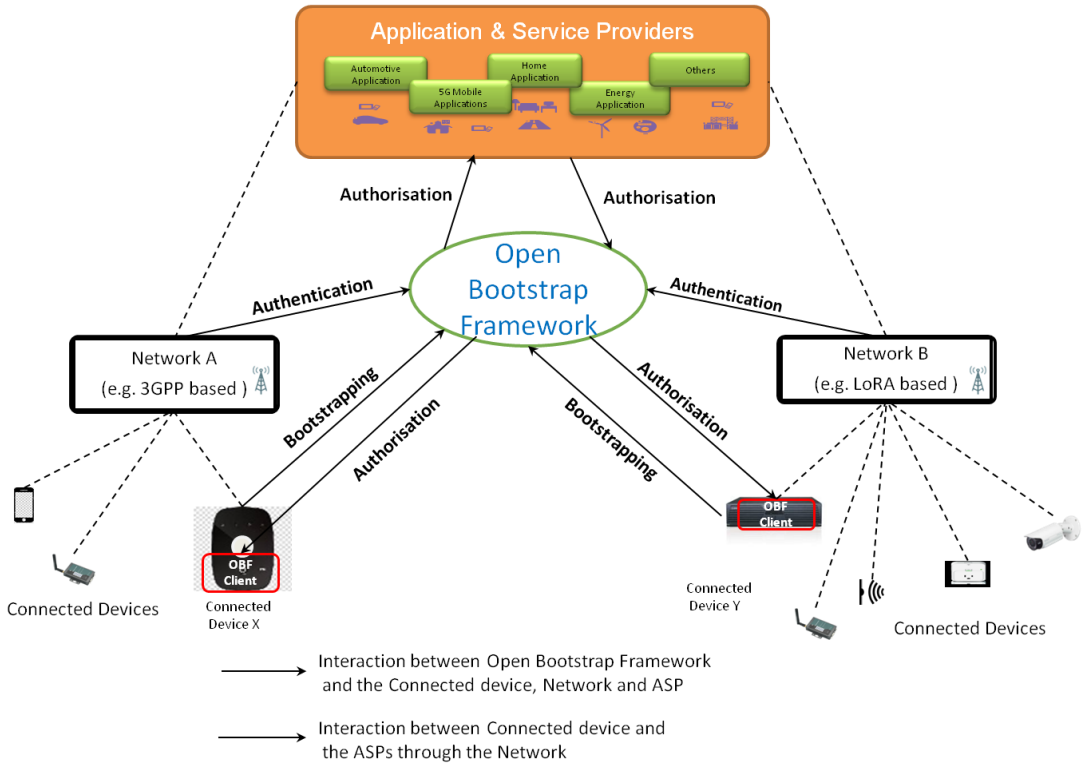

Figure 3: Working Model of the OBF

6.4 OBF Functional Architecture

The functional realization of the OBF is provided in the form of a functional architecture. The OBF Services are exposed by the orchestration of three OBF nodes and four reference points, which are shown in the Functional Architecture diagram below:

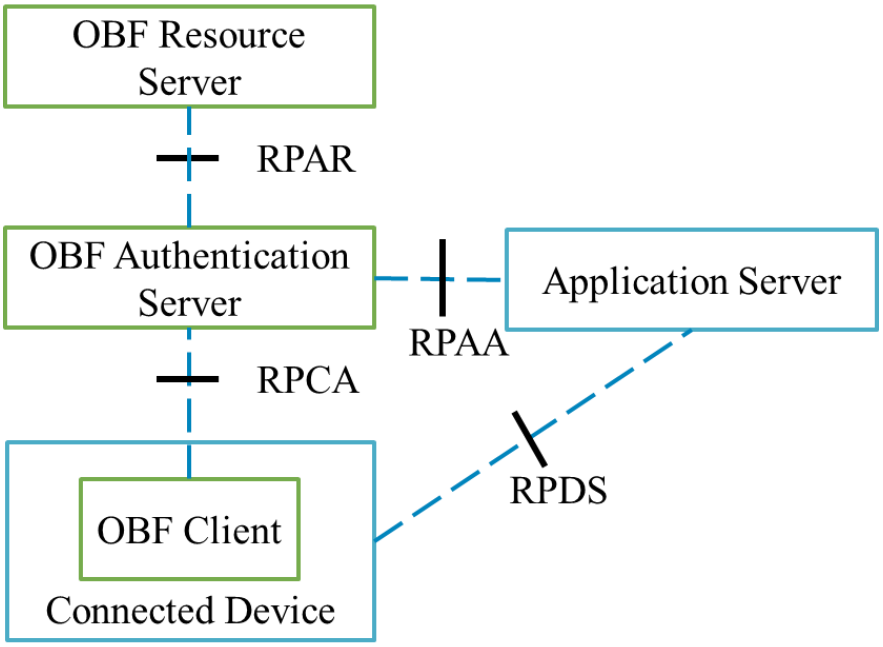

Figure 4: Functional Architecture showing the OBF Elements

The OBF Functional Architecture consists of three nodes and four reference points. The Connected Device and the Application are the beneficiaries of the Trust Framework, but not a part of the OBF. The software elements, namely, the OBF Client, OBF Authentication Server and the OBF Resource Server are the nodes of the Functional Architecture. The nodes interact with each other using four reference points, namely, RPAA, RPAR, RPCA and RPDS.

NOTE: To specify the processes such as Trusted Application Provisioning is out of scope of this Recommendation, as these are controlled by policies and governance mechanisms on the related market, actors and ecosystems.

_____