INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION STANDARDIZATION SECTOR**

STUDY PERIOD 2017-2020

**Q16-13-May20-C118R2**

**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<br>Telecom Engineering Centre (TEC)<br>India | Tel: + 91 9868138506<br>E-mail: as.verma@gov.in |
| **Contact:** | Ranjana Sivaram<br>Telecom Engineering Centre (TEC)<br>India | Tel: +91 9868136990<br>E-mail: ranjana.sivaram@gov.in |
| **Contact:** | Sharad Arora<br>Sensorise Digital Services Pvt Ltd<br>India | Tel: +91 9212109999<br>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

Users of new age services require mechanisms for trusted access to reliable Services. At the same time, providers of trusted applications and services also require mechanisms for a minimum level of authentication of the Users. Open bootstrap framework enables secure interactions between Users and Connected Devices on the one hand, and the Applications and Service Providers on the other, by utilizing the inherent security capabilities of the underlying network technology layer.

From time immemorial, the Network Operators have 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.

The OBF recommendation makes it possible to extend the existing trust relationship between the network operator and its subscribers to enable one to many trust relationships between the users and the many new age service providers.

The OBF defines a set of functions, requirements, capabilities and mechanisms that open up the security capabilities of the network layer to all types of connected devices, applications and services. The OBF can be implemented by Network Operators providing any type of network that permits bootstrapping of devices. Further, any user of a bootstrapped device can access the applications and services of any ASP by using the OBF functions and mechanisms. The OBF is a trust framework, which opens up and extends the existing trust relationship between the user and the Network Operator to be utilized by an ASP for providing trusted services to hitherto unknown user of a connected device.

The OBF addresses the critical need for an inter-operable, network technology agnostic framework for sharing of trust between the Network Operator, ASP and the User by bootstrapping of connected devices, authentication of users and authorization of applications based on the trust provided by the Network Operator.

The Users and their Connected Devices are authenticated based on the bootstrapping provided by the Network Operator that provides the network layer security and access control. ASPs 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.

The OBF provides an interoperable, implementation-independent and scalable approach for multi-party interactions in which a diverse set of connected devices using a variety of network technologies are able to access applications and services securely. 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.

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.

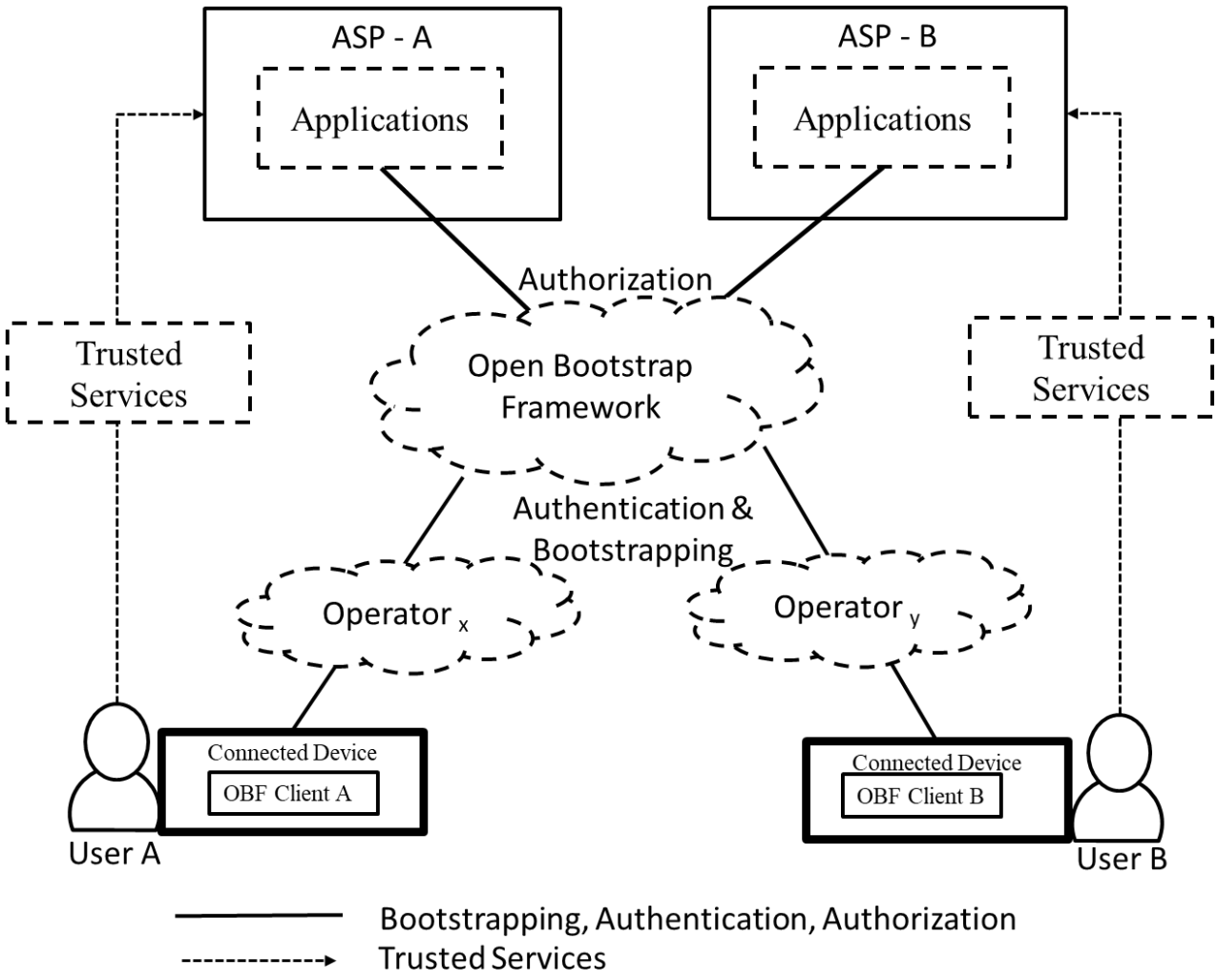


**Figure 1: OBF Concept**

The OBF provides for the following functions:

1. **Bootstrapping of Connected Devices**

The bootstrapping function provides a strong mutual authentication of a connected device to the authentication server by the use of the security capabilities of the secure element.

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

The 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 Applications and Services

The 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.