INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG13-TD394/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Geneva, 13 March 2020

TD

Source: Editors

Title: Draft Recommendation ITU-T Y.OBF_trust: “Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems”

Purpose: Information

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: Authorisation Function; Authentication Provider; Authentication Framework; Bootstrapping; Connected Services; Constrained Devices; Machine KYC; Machine to Machine Service Provider; OBF (Open Bootstrap Framework); OBF Proxy; OBF Key Management System; RADIUS; Resource Server; Root of Trust; Secure Element; Session Keys; Symmetric keys; Third Party Service Providers; Trust Framework

Abstract: This document contains the updated draft Recommendation ITU-T Y.OBF_trust “Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems” based on the discussion at Rapporteur Group meeting of Q16/13 (2-13 March 2020, Geneva) based on the contribution C91.

This document is the revised baseline text of draft Recommendation ITU-T Y.OBF_trust:” Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems” This document is based on following contribution.

No.	Source	Contribution title and proposals	Agreements
C91	India	Draft Recommendation ITU-T Y.OBF_trust: “Open Bootstrap Framework enabling	The contribution was agreed.

		trustworthy networking and services for distributed diverse ecosystems” Proposals: This document proposes to update the draft Recommendation ITU-T Y.OBF_trust by adding the content in Annexure - I to the corresponding clauses viz. Clause 3.2, Clause 9.1.3, Clause 9.3, 9.3.1 and 10.2.4	

Draft Recommendation ITU-T Y.OBF_trust

Open Bootstrap Framework enabling trustful devices, applications and services for distributed diverse ecosystems

Summary

Draft Recommendation ITU-T Y.OBF_trust describes an Open Bootstrap Framework (OBF), which includes an OBF Client, an OBF Authentication Server, an OBF Resource Server and four Reference Points. It unfolds a bootstrapping architecture and a description of the OBF elements, reference points, mechanisms and workflows for the mutual authentication between Connected Devices, Applications and Service Providers.

The objective of the OBF is to provide security bootstrapping to devices for the purpose of extending trustful services to any Application/ Service Provider by re-using the Secure Element and trustful networking capabilities of the network technology layer.

The Recommendation is relevant to Network Operators, M2M Service Providers and Applications/ Services Providers for deployment of secure services in the emerging 5G/ Smart Cities/ IoT Application/ Services domain.

Keywords

Authorisation Function, Authentication Provider, Authentication Framework, Bootstrapping, Connected Services, Constrained Devices, Machine KYC, Machine to Machine Service Provider, OBF (Open Bootstrap Framework), OBF Proxy, OBF Key Management System, oneM2M, RADIUS, Resource Server, Root of Trust, Secure Element, Session Keys, Symmetric keys, Third Party Service Providers, Trust Framework

Contents

Draft new Recommendation ITU-T Y.OBF_trust

Open Bootstrap Framework enabling trustful devices, applications and services for distributed diverse ecosystems

1 Scope

This draft Recommendation specifies an Open Bootstrap Framework that allows the Registration, Authentication and Authorisation between Devices (including Constrained Devices), Connected Services, Service Providers and Applications.

The scope of this draft Recommendation includes

- A Concept that extends the use of embedded Secure Elements and Keys, originally intended for Operator Services, to be used for creating secure associations for Applications provided by Third Party Service Providers
- An Open Bootstrap Framework with definitions of Nodes and Reference Points
- A set of functions, mechanisms and workflows for securitising the interactions between the stakeholders in the physical world and the services in the cyber space

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1113] Recommendation ITU-T X.1113 (2007), *Guideline on user authentication mechanisms for home network services*

[ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device*

[ITU-T Y.2724] Recommendation ITU-T Y.2724 (2013), *Framework for supporting OAuth and OpenID in next generation networks*

[ITU-T Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning for information and communication technology infrastructures and services*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1. Authentication servers [ITU-T X.1113 (11/2007)]: Authentication servers refer to servers that provide authentication services to users or other systems. Authentication is generally used as the basis for authorization (determining whether a privilege will be granted to a particular user or process), privacy (preventing the disclosure of information to non-participants), and non-repudiation (not being able to deny having done something that was authorized to be done based on the authentication).

3.1.2. **Resource server** [ITU-T Y.2724 (11/2013)]: The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.

3.1.3. **Secure element** [ITU-T X.1158 (11/2014)]: A dedicated microprocessor system that contains an operating system, memory, application environment and security protocols intended to be used to store sensitive data and execute sensitive applications.

NOTE – A secure element may reside in a universal subscriber identity module (USIM), a dedicated chip in a phone's motherboard, an external plug in a memory card or as an integrated circuit card.

3.1.4. **Session key** [ITU-T X.1113 (11/2007)]: The session key is a temporary key used to encrypt data for the current session only. The use of session keys keeps the secret keys even more secret because they are not used directly to encrypt the data. Secret keys are used to derive the session keys using various methods that combine random numbers from either the client or server or both.

3.1.5. **Trust** [ITU-T Y.3052]: Trust is the measurable belief and/or confidence which represents accumulated value from history and the expecting value for future.

Note – Trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of entities, value-chains among multiple stakeholders, and human behaviours including decision making.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1. **Bootstrapping**: Refers to a process performed in a secure context prior to the deployment of the connected device to establish a security association between the connected device that may have been initialized with credentials, enabling a connected device to communicate securely with other connected device after their deployment.

3.2.2. **Connected Device**: A device that has an embedded secure element in itself or its Connectivity Element.

3.2.3. **Constrained Device:** A device with limited processing and compute and/ or storage capabilities due to limited battery life and also having limitations to cryptographic capabilities.

3.2.4. **IDP:** Identity Provider, a service that can be used to allow multiple applications to use the service for authentication using a single Identity. (Single Sign-On)

3.2.5. **M2M service provider:** Entity (e.g., a company) that provides M2M Services to an M2M Application Service Provider or to the User.

3.2.6. **Machine KYC:** The Process of establishing a relationship between a machine and its custodian, usually accomplished by either, the use of third-party verification or digital identity verification

3.2.7. **OBF:** is a trust framework for extending the security capabilities of any network technology to benefit third party devices and applications.

3.2.8. OBF_Token: A session key generated in the Connected Device/ User Equipment (UE) by the Authentication Function for establishing a secure association between Applications of the Connected Device and the Application Server.

3.2.9. Operator Services: Services provided to the user of a Connected Device, that are offered by and hosted in the network of the Network Service Provider e.g. MNO

3.2.10. Resource Server: A Server that holds / hosts the protected user resources

3.2.11. RPR: Reference point where the Authentication Server can get the resource rights for a certain device

3.2.12. RPO: Reference point used by the Application Server to fetch key material from the Authentication Server. It is also used to fetch application-specific user security settings from the Authentication Server if requested

3.2.13. RPB: The reference point is between the Secure Element and the Authentication Server. The Reference point provides mutual authentication between the Secure Element and Authentication Server. It allows the Secure Element to bootstrap the session keys

3.2.14. RPA: The reference point carries the application protocol, which is secured using the keys material agreed between Secure Element and Authentication Server

3.2.15. Secure Element: A tamper-proof component, within or outside the device or the connectivity element serving the device, that has the capability to store data of the keys required for the security function and run at least one authentication algorithm.

3.2.16. Third Party: An entity other than the network provider, which consumes network capabilities of a network for providing applications and/ or services to the end users.

3.2.17. Trust framework: A system where a set of verifiable commitments are made by each of the various parties in a transaction to their counter parties, and these commitments necessarily include: (a) controls to help ensure commitments are met and (b) remedies for failure to meet such commitments.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSF	Bootstrapping Server Function
eUICC	Embedded UICC
EID	eUICC-ID
HLR	Home Location Register
ICT	Information and Communication Technology
IoT	Internet of Things
KYC	Know Your Customer
M2M	Machine to Machine
M2M SP	M2M Service Provider
MNO	Mobile Network Operator
NAF	Network Application Function
OBF	Open Bootstrap Framework

SE	Secure Element
SIM	Subscriber Identification Module
SLF	Subscriber Locator Function
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TSP	Telecom Service Provider, see also MNO
UICC	Universal Integrated Circuit Card

5 Conventions

In this Recommendation, requirements are classified as follows:

- The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed;
- The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, such requirements need not be present to claim conformance; and
- The keywords "**can optionally**" and "**may**" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option; it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction and Overview of the Open Bootstrap Framework

The OBF uses a unique identity in a tamper resilient hardware that can act as a root of trust, providing the required identity for authentication of remote and dispersed devices, applications and actors in an ICT enabled business value chain. By adding the required Key Management, Authentication and Authorization functions, a bootstrapping framework is defined that makes it possible for any application and service provider to provide a higher degree of security to the User and Services.

A reference model for such an Open Bootstrap Framework (OBF) is defined below.

6.1 OBF Reference Architecture

The elements of the proposed OBF reference model are shown in the diagram below.

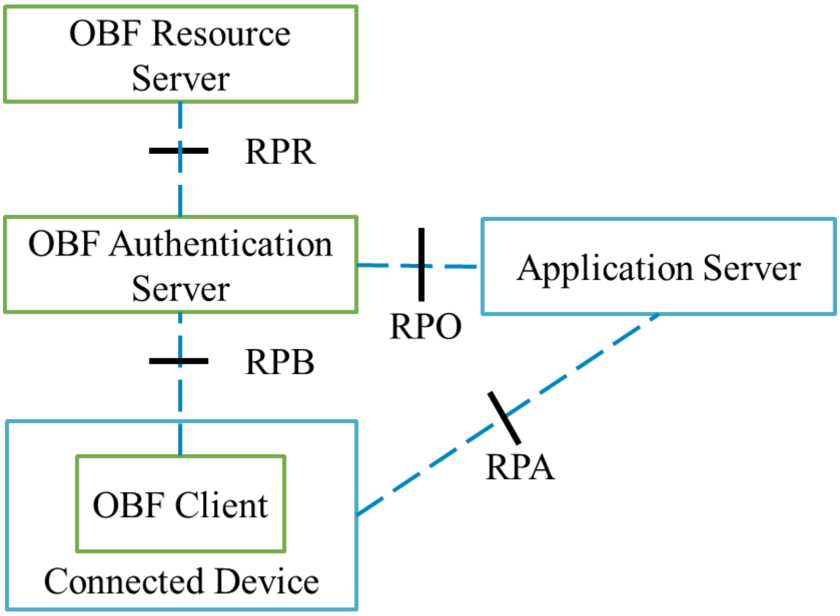


Figure 1: OBF Reference Architecture

The elements of the reference architecture consist of three nodes and four reference points. The Connected Device and the Application are the beneficiaries of the OBF, but not a part of the OBF. The software elements, namely, the OBF Client, OBF Authentication Server and the OBF Authorisation Server are the nodes of the reference model. The nodes interact with each other using four reference points, namely, RPO, RPR, RPA and RPB.

When the elements of the reference architecture work together with the beneficiary Connected Devices and Applications as per the mechanisms and workflows defined for the OBF, they create a trust framework which is described below.

6.2 OBF Trust Framework

The OBF trust framework is a set of relationships and interactions between actors in the Physical and Cyber domain, who use the elements of the OBF, and a set of defined mechanisms and workflows, to achieve the objective of enhanced trust and security.

The concept of the trust framework created by the OBF is shown in Figure 2. The framework shows two domains, namely, the Operator Domain, the Third-Party Service Provider Domain. The trust framework has two operating spaces – the Physical and the Cyber space. The Actors in the OBF trust framework are the Network Service Providers such as the MNOs and M2M SPs; Applications and Services Providers that provision ICT-enabled Services and the User community that buys and uses the ICT-enabled Services.

By following the OBF recommendations, the actors in the Physical space are able to derive a trustful relationship between themselves, the Connected Devices and the ICT-Enabled Applications.

The Figure 2 shows the interactions between the elements of the OBF, and the Actors in the Physical and the Cyber Space. The trust framework enables identification, authentication and authorization for the use of Connected Devices and Applications, using mechanisms and workflows which are more fully described in the sections below.

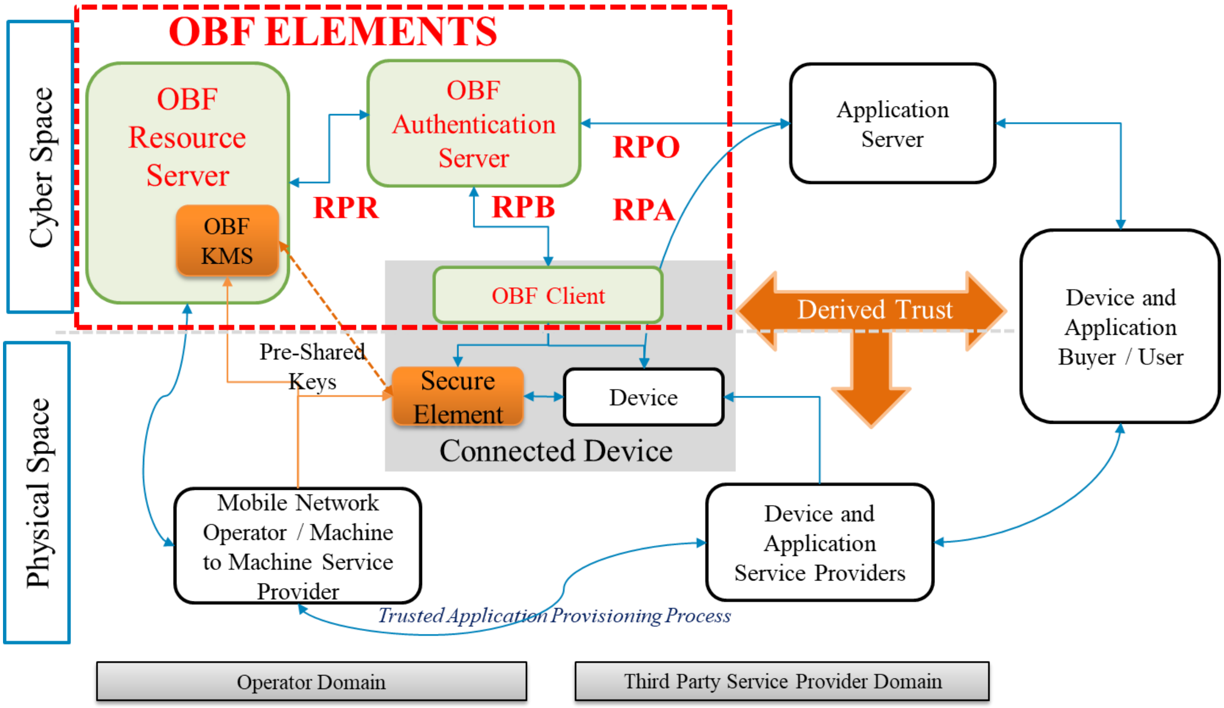

OBF ELEMENTS
Cyber Space
Physical Space
OBF Resource Server
OBF KMS
OBF Authentication Server
RPR
RPB
RPO
RPA
Application Server
OBF Client
Derived Trust
Device and Application Buyer / User
Pre-Shared Keys
Secure Element
Device
Connected Device
Mobile Network Operator / Machine to Machine Service Provider
Device and Application Service Providers
Trusted Application Provisioning Process
Operator Domain
Third Party Service Provider Domain

Figure 2: Trust Framework using OBF Reference Model

It is not in the scope of this document to specify the processes such as Trusted Application Provisioning as these are controlled by policies and governance mechanisms on the related market, actors and ecosystems.

7 OBF Elements

The OBF specifies the OBF Client, OBF Nodes and OBF Interfaces, each of which is described below.

7.1 OBF Nodes

The OBF specifies three Nodes, each of which is described below:

7.1.1 OBF Client

The OBF Client is an application resident in the Connected Device or the Connected Device Connectivity Element that provides the bootstrapping application and the key material on the device side for the bootstrapping of the Connected Device using the Authentication Function. The OBF Client provides the features and functions required for the interaction with the Authentication Server and Application Server. The OBF Client is specified and provisioned by the M2M Service Provider or the Mobile Network Operator that is providing the OBF services.

7.1.2 OBF Resource Server

The OBF Resource Server is a network node that provides the key material on the Service Provider side for the bootstrapping service provided by the Authentication Server. The OBF Resource server hosts the required Key Management Systems.

The OBF Resource Server is specified and provisioned by the M2M Service Provider or the Mobile Network Operator that is providing the OBF services.

7.1.3 OBF Authentication Server

The OBF Authentication Server is a network node that mutually authenticates the OBF Client towards the OBF Resource Server, generating in the process, a set of algorithms and keys that are then used for the security of the transactions between the Connected Device and the Application Server that is hosting the Connected Services.

7.2 OBF Reference Points

The OBF specifies four Reference Points, each of which is described below:

7.2.1 RPB

The Reference Point is between the OBF Client hosted in the Secure Element and the OBF Authentication Server. The Reference point provides mutual authentication between the OBF Client in the Secure Element and OBF Authentication Server. It allows the OBF Client in the Secure Element to bootstrap the Connected Device and the Connected Service using session keys. The recommended protocol to be used over RPB is HTTP Digest protocol [b-RFC7616], the interface between the Connected Device and the Secure Element is as per the specifications of the underlying Network Technology.

7.2.2 RPO

The Reference Point between Authentication Server and Application Server. It is used by the Application Server to fetch key material from the Authentication Server. It is also used to fetch application-specific user security settings from the Authentication Server if requested. The recommended protocol to be used over RPO is RADIUS [b-RFC 2865] with the addition on TLS [b-RFC6614].

7.2.3 RPR

The Reference Point between OBF Authentication Server and OBF Resource Server. Here the OBF Authentication Server can get the resource rights for a certain Connected Device. The recommended protocol to be used over RPR is RADIUS [b-RFC 2865].

7.2.4 RPA

The Reference Point is between the Connected Device and the Application Server. It carries the application protocol, which is secured using the keys material agreed between OBF Client hosted in the Secure Element and the OBF Authentication Server. The communication protocol between the Connected Device and the Application Server is not in the scope of this recommendation.

7.3 OBF_Token

It is a session key generated in the Connected Device/ User Equipment (UE) by the Authentication Function for establishing a secure association between Applications of the Connected Device and the Application Server.

OBF_Token shall be derived either from the device or secure element by using device identification, Secure key material, connectivity information, and time stamp/ counters.

8 Capabilities of OBF

8.1 Overview of Capabilities of the OBF

The capabilities of OBF are as follows:

- The OBF Key Management System is able to create and upload Keys to the OBF Resource Server and the OBF Client, where the underlying Network Technology requires the creation of keys by an external element;
- The OBF Key Management System is able to ingest keys, where the underlying Network Technology creates the keys;
- Register the Resource Servers and the Resource Server Providers (MNOs and M2M Service Providers);
- Register the Application Servers and the Application Service Providers;
- Initiate the bootstrapping process to create a repository of trusted Connected Devices;
- Provision Application Service provider applications towards Connected Devices;
- Transfer Connected Devices between Authentication Service Providers such as MNOs, and M2M SPs; and
- Support Functions and Flows as specified below.

8.2 Functions

Authentication Functions implemented in the Secure Element, Device and the Servers (namely, Resource, Authentication and Application Servers), which are involved in the Authentication process, are is required to be as follows:

8.2.1 The Authentication Function

This function is hosted in the network of the MNO/M2MSP under the control of the issuer of the Secure Element. The Authentication Server, Resource Server, and Secure Element participate in Authentication procedure in which a shared secret is established between the Authentication Server and the OBF Client hosted in the Secure Element by running the bootstrapping procedure over the reference point RPB as described in the OBF Authorisation Function below.

8.2.2 OBF Client Function:

A function of the OBF Client hosted in the Secure Element that executes the bootstrapping procedure with the Resource Server and Authentication Server and provides the Connected Device with security association to run bootstrapping usage procedure.

8.2.3 Connected Device Function:

An Application calls this function over the reference point RPA when an application server requires a bootstrapped security association.

8.2.4 OBF Authorisation Function:

The OBF Authorisation Function resides in the OBF Resource Server and validates if the OBF_Client has the right to use the authentication for the requested application/service. It is the repository of registered Applications that can be permitted for use by the Device / User that is registered with the OBF Authentication Server. The OBF Authorisation Server maps the Application Identities to the OBF_Token issued to the User by the Authentication Function.

9 Requirements

The OBF may be deployed by an MNO or an M2MSP. The requirements for the Open Bootstrap Framework are identified in the clauses below:

9.1 Requirements of usability by various actors

The OBF implementation is required to confirm that:

- Open accessibility of the OBF for use by any Connected Device and Applications offered by any of MNO, M2MSP or Third Party Service Providers;

- The OBF ensures that the end user or buyer can freely choose services from any MNO, M2MSP or Third Party Application Service Providers without affecting the Authentication Services offered by the OBF; and

- To ensure compatibility with various Networking Technologies, the OBF to identify the Network Technology, and provide the Authentication Services using the global identities, key material and crypto algorithm as per the underlying Network Technology layer.

9.2 Requirements of trust model for authentication services

The OBF implementation is required to confirm that:

- Provide a trust model which represents the Physical, Cyber and Trust domains and the involved resources and stakeholders including their relationships; and

- The Applications permitted to be accessed by Connected Devices be provisioned on the Resource Server.

9.3 Requirements of OBF Identifiers and Key Management

The OBF implementation is required to confirm that :

- Presence of a Secure Element in the Connected Device or its Connectivity Element;

- The OBF offers Authentication Services using the global identities as per the underlying Network Technology layer without any change;

- The use of Pre-Shared Keys or Public Key Infrastructure, as part of the Network Technology layer authentication service, is a pre-requisite for the proper functioning of the OBF;

- Commonly agreed set of Security Algorithms is required to simultaneously co-exist on the Secure Element and the OBF Key Management System; and

- OBF_Token :

- be globally unique;
- be usable as a key identifier in protocols used in Reference point RPO; and
- be able to provide adequate information to the OBF Authentication Server to make it capable of detecting the domain and the OBF Resource Server of the Connected Device.

9.4 Requirements for the RPA Interface

It is required to fulfil that:

- The OBF Client and the Third-Party Application Server support the HTTP Digest protocol [b-RFC7616];
- The Connected Device has an implementation to communicate with the Secure Element;
- The Third-Party application running on the Connected Device signals to the OBF Clinet (Secure Element) when it requires to use the OBF; and
- The Application Server and the Connected Device application use the OBF_Token to create new sessions.

9.5 Requirements for the RPB Interface

It is required to fulfil that:

- The registration and identification of the OBF Client (Secure Element), and the Connected Device that the Secure Element is attached to, is done by the Authentication server;
- The mechanism for mutual authentication between the Authentication Server and OBF Client (Secure Element) is implemented; and
- The mechanism for transfer of the OBF_Token from the Authentication Server to the Application Server is established.

9.6 Requirements for the RPO Interface

It is required to fulfil that:

- The mechanism for the secure communication between the Application Server and the Authentication Server is implemented; and
- The mechanism for transfer of the OBF_Token from the Authentication Server to the Application Server is established.

9.7 Requirements for the RPR Interface

The Resource Server is required to provide the Authentication Server with relevant data to be shared with an Application Server.

10 Pre-requisites for Devices, Application and Resource Servers

10.1 Device Pre-requisites

It is required that the following constraints are to be fulfilled by the Devices that make use of the OBF

- Presence of the OBF Client and the Secure Element in the Connected Device or its Connectivity Element;

- Support for interface between the Connected Device and the Secure Element as per the specifications of the underlying Network Technology; and

- Support for one or more protocols - HTTP, MQTT, Web Sockets or COAP.

10.2 Application Server Pre-requisites

It is required that the following constraints are to be fulfilled by the Application Servers that make use of the OBF:

- Support for one or more protocols - HTTP, MQTT, Web Sockets or COAP, which are used by the Devices in the ecosystem; and

- Ability to set local validity conditions of the shared key material according to the local policy;

- Ability to honour lifetime and local validity condition of the shared key material.

It is recommended that support for new protocols are added as and when released within the relevant ecosystem.

11 Operations and Mechanisms

The following Operational Workflows are defined for the OBF

11.1 Authentication Workflow

The Authentication Workflow is meant for a User that would like to use a Service or an Application that can benefit from the OBF Authentication.

When a User requires to access an application from the Connected Device, or the Application requires to exchange data with the Application Server, the application signals to the OBF Client the requirement to use the bootstrap framework for authentication. This process in accomplished in the following steps:

1. Bootstrapping is initiated, if it has not been executed previously. The bootstrapping itself can be done either using pre-shared keys, or by using asymmetric keys.
2. The resource server validates if the User has the right to use the authentication for the given application. To end the bootstrapping stage, the Authentication Server and OBF Client agree on a OBF_Token [session key material] to be used upon successful verification.
3. The User request towards the Application server is executed and the application will run the challenge it deems fit (not in the scope of this recommendation) to identify the User.
4. User responds to the Challenge thrown by the Application
5. Application Server issues a challenge to the Authentication Server

6. Upon successful completion of the steps 4,5 the Authentication Server will provide OBF_Token [session key material] that was previously agreed on between the OBF Client and Authentication Server. The OBF_Token [session key material] is used to set up a TLS secure connection for any data exchange between the Connected Device application and the Application Server.

The Workflow is described in the diagram below:

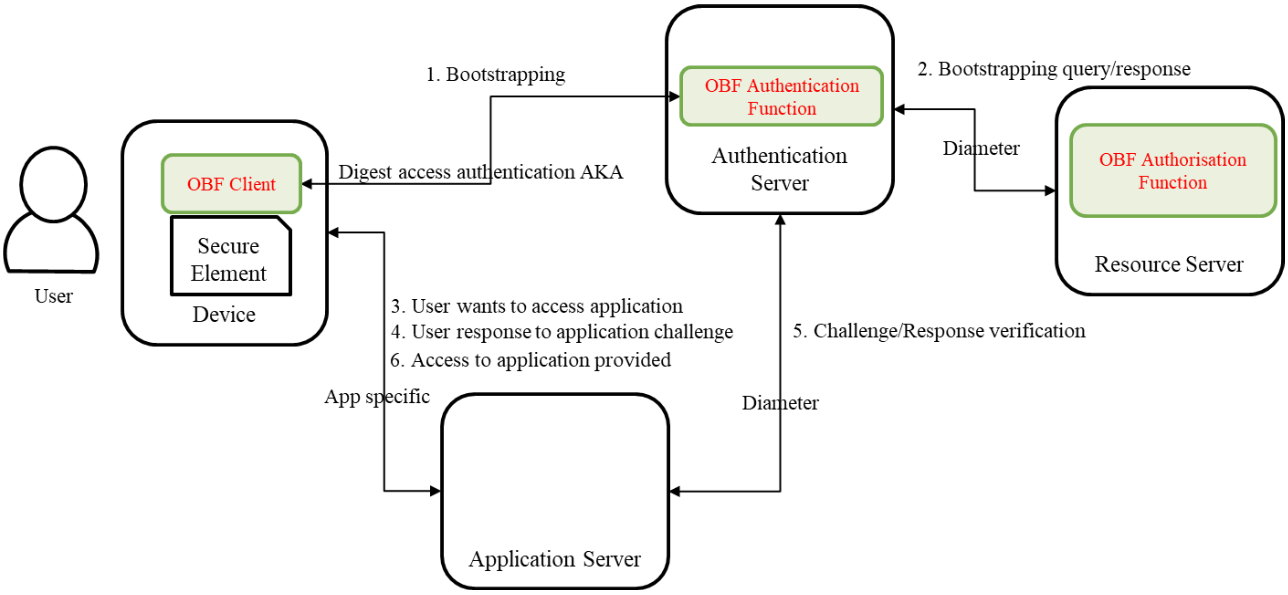

1. Bootstrapping
OBF Authentication Function
Authentication Server
2. Bootstrapping query/response
Diameter
OBF Authorisation Function
Resource Server
OBF Client
Digest access authentication AKA
Secure Element
Device
User
3. User wants to access application
4. User response to application challenge
6. Access to application provided
5. Challenge/Response verification
App specific
Diameter
Application Server

Figure 3: Authentication Flow

11.2 Key Management during bootstrap Flow

The shared key that exists on both the Secure Element, and in the Key Management System of the Authentication server, is used to authenticate the OBF Client with the Authentication Server. Session Keys are used for securing the communication between the device and an Application Server. The figure below shows how these Session Keys are managed:

1. The Authentication Server will validate the client in the bootstrapping stage
2. The Authentication Server and the OBF Client will mutually challenge each other to validate credentials
3. When the mutual authentication has completed the OBF Client and Authentication Server agree on the OBF_Token [session key material] (how the session key is generated is not in scope of this recommendation).
4. User tries to access the Application Server
5. The Application verifies the user with the OBF_Token [session key material]

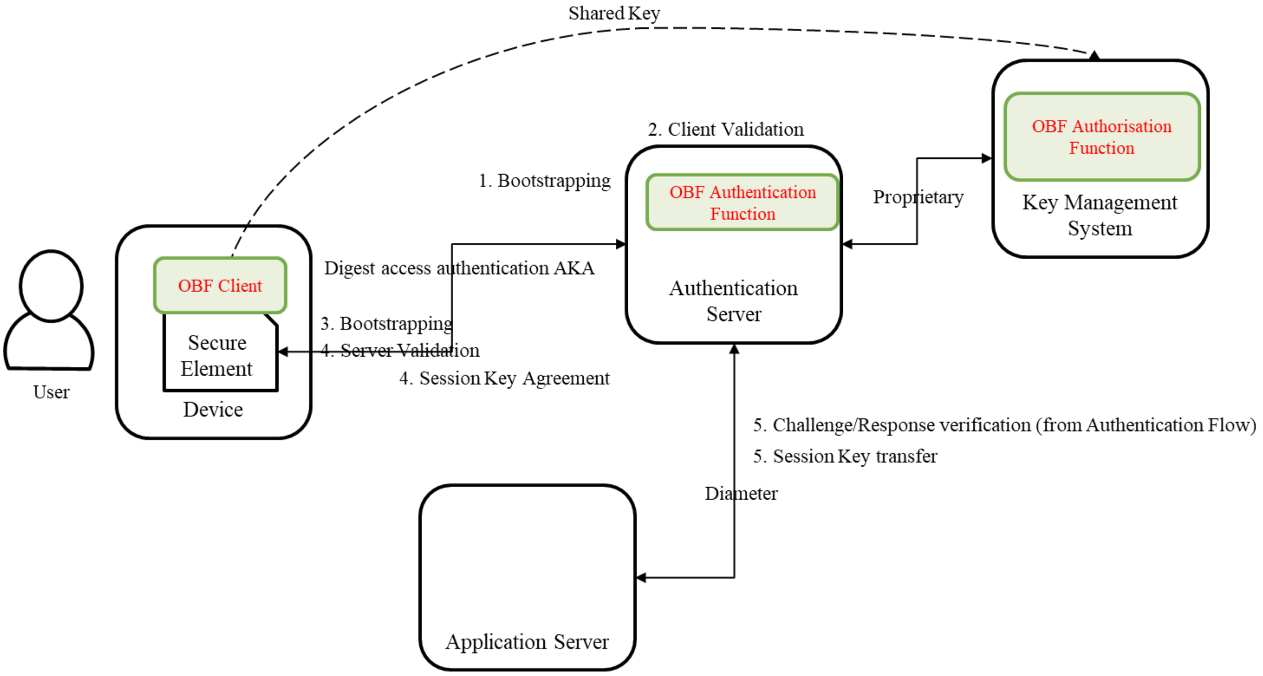


Figure 4: Key management during bootstrap

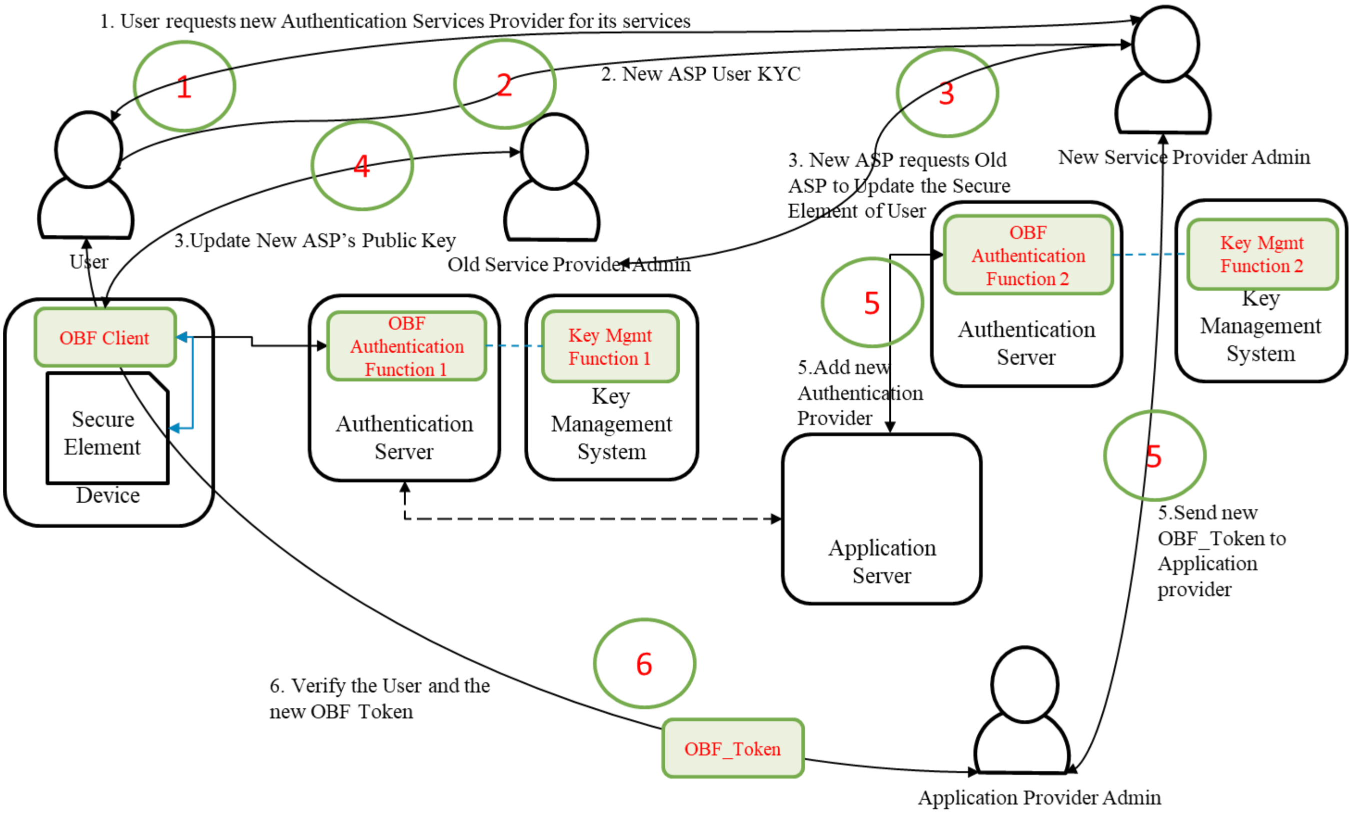
11.3 Changing of Authentication Provider Flow (Asymmetric keys)

A User may change the Connectivity Provider, but still may want to continue the use of Services which are supported by the OBF Authentication. The Authentication Provider may be changed as per the mechanism defined below:

A User may wish to change the Connectivity Provider, but retain the use of Applications which are supported by the OBF Authentication. When using Asymmetric Keys, the Authentication Provider may be changed as per the mechanism defined below:

1. User requests new Authentication Services Provider for its services
2. The new Authentication Services Provider completes the User KYC
3. The new Authentication Service Provider provides its Public Key to the old Authentication Service Provider with a request to transfer the User's Account to the new Authentication Service Provider
4. The old Authentication Services Provider uses its Private Key to update the Secure Element of the User with the Public Key of 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

Figure 5: Authentication Provider Switch (Asymmetric keys)


1. User requests new Authentication Services Provider for its services
1
2
2. New ASP User KYC
3
4
New Service Provider Admin
3. New ASP requests Old ASP to Update the Secure Element of User
3.Update New ASP's Public Key
User
Old Service Provider Admin
OBF Authentication Function 2
Authentication Server
Key Mgmt Function 2
Key Management System
5
5.Add new Authentication Provider
OBF Client
Secure Element
Device
OBF Authentication Function 1
Authentication Server
Key Mgmt Function 1
Key Management System
Application Server
5
5.Send new OBF_Token to Application provider
6
6. Verify the User and the new OBF Token
OBF_Token
Application Provider Admin

11.4 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. The Steps for such a transfer are described below

1. : 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:

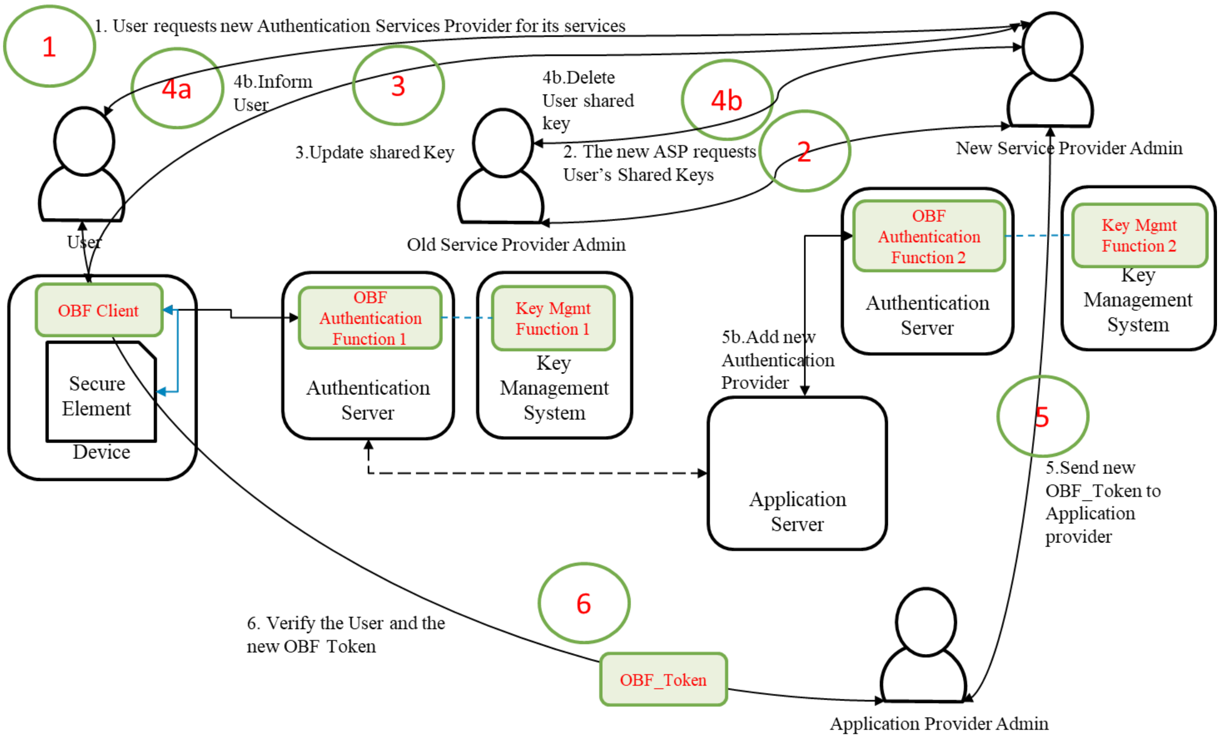

1
1. User requests new Authentication Services Provider for its services
4a
4b.Inform User
3
3.Update shared Key
4b.Delete User shared key
4b
2
2. The new ASP requests User's Shared Keys
New Service Provider Admin
User
Old Service Provider Admin
OBF Client
Secure Element
Device
OBF Authentication Function 1
Authentication Server
Key Mgmt Function 1
Key Management System
OBF Authentication Function 2
Authentication Server
Key Mgmt Function 2
Key Management System
5b.Add new Authentication Provider
Application Server
5
5.Send new OBF_Token to Application provider
6
6. Verify the User and the new OBF Token
OBF_Token
Application Provider Admin

Figure 6: Change Authentication Service Provider (Symmetric Keys)

Appendix I

Real-world explanation of the use case example

(This appendix does not form an integral part of this Recommendation.)

This appendix provides real-world explanation of the use case examples of OBF. In this use case, the background, the device functions and the sample data flow has been described.

I.1 Background and Diversified multi-stakeholder eco system

The Ecosystem comprises of the following Actors

a. MNO or M2MSP: Supplier of the SIM and Secure Element
b. Device Manufacturer – manufacturer of the Device with the embedded SIM / Secure Element
c. Vehicle Manufacturer – manufactures of the vehicle with the embedded device, SIM and Secure Element
d. Buyer – the entity or person that pays for the Vehicle
e. Application Provider – the entity that provides the Application for registration, tracking and transfer of the vehicle
f. Certifying Agency – the entity that Certifies the Device and the Application
g. Trust Centre – the Agency responsible for the registration and enforcement of Vehicle rules, typically a State actor

I.1.1 Background

The use case is a real-world use case in India “see clause I.1.2”. Indian automotive standard body has laid down a Standard (Automotive Indian Standard AIS140) for the registration and tracking of public service vehicles, including the communication between Vehicle Tracking Device (VTS) and a Vehicle Tracking and Alarms Management Server (VTAMS)

As per this standard, the VTS device sends various data packets to the VTAMS server like Position-Velocity-Time Data, Panic Alarm, Safety Alerts, Health Data, Diagnostics etc. VTAM Server controls the devices by sending various commands to VTS device; like get device diagnosis, configuration command, Panic Alarm Acknowledgement, Panic Alarm Closure etc. Communication from device to server and server to device is taking place over SMS and TCP/IP channel.

Given the mission critical nature of the service, the VTAMS server is having mechanisms to establish the Integrity, Identity, Authenticity and Trust to ensure the secure and trustful implementation of public safety for the citizens.

I.1.2 Diversified multi-stakeholder eco system

In continuation of background, it is also important to describe the diversified eco system which will enable the AIS140 standard in India.

1. There are more than 40 VTS device manufacturer who are supplying the VTS devices for Public Transport Vehicles
2. Few device manufacturers are designing and manufacturing the devices from ground up and few are assembling the devices and controlling the firmware only. May devices are constrained devices and are designed for specific purpose only.

3. There are 4 major MNOs (Mobile Network Operators) providing the communication channel.
4. There are multiple M2M Service Providers, providing the end to end services
5. There are multiple SIM Manufacturer, supplying the SIM Cards to M2M SP or OEM Directly
6. There are more than 30 States that will implement their own Application Servers at the State Data Centres
7. There are dozens of Application Service Providers who will license the Tracking and Alarms Management Systems to individual States

I.2 Use case

This use case is for Remote Manageable basic vehicle tracking devices (without crypto functionality) with embedded SIM (Secure Element). In this use case, device is sending health, diagnosis and other data to national backend system (Application Server). Device is also receiving configuration change command (like application server IP change) from National Backend System (Application Server).

When device is sending data to National Backend System (Application Server), then:

1. Application server is able to identify the device correctly
2. Application server is able to check the data integrity which means no one in between have changed the data
3. Application server is be able to identify replay attack from a malicious entity
4. No one in between device and application server should be able to read the data being sent by device

Similarly, when National Backend System (Application Server) is sending command, like application server address change, to device:

1. Device is able to identify that this request is coming from authorized application server
2. Device is able to check the data integrity which means no one in between have changed the data
3. Device is able to identify replay attack from a malicious entity
4. No one in between application server and device should be able to read the data being sent

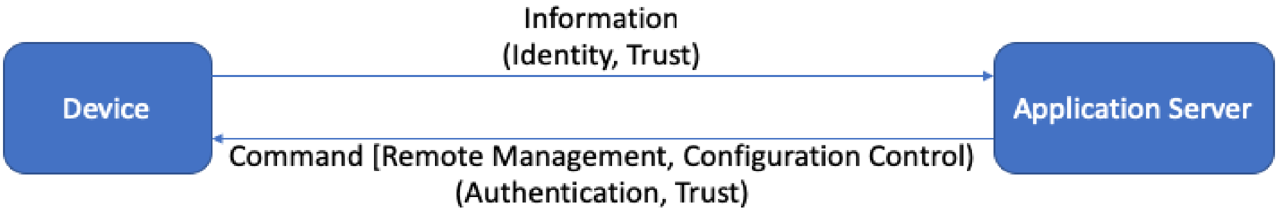


Figure I.1: Device-Application Server Communication

I.2.1 Important consideration for security

Following are important consideration for security implementation:

1. The tamper proof identity of the SIM / Secure Element (IccID / EID) is used as the primary identifier for the connected device
2. Appropriate mechanisms are followed for the generation and sharing of Security key between the SIM / Secure Element and the Authentication Server
3. The NAF and the OBF interact securely following the standards prescribed by 3GPP GAA.

I.2.2 Functions required

Following functions are required on device, secure element and application server to meet the mentioned security requirement “see clause I.2.1”:

I.2.2.1 Device Functions

I.2.2.1.1 Validate Checksum Function

This function is used by device to validate the checksum of the incoming data. This will ensure the **Data Integrity**. If checksum is not matched, then device will not process the data further and ignore it.

I.2.2.1.2 Decrypt Encrypted Server Data Function

When Device receives data from an application server (like configuration change command), it will first establish the data integrity. Once the data integrity is established, the M2M device will send the data to Secure Element for decryption.

The purpose of the function is to authenticate the Application Server to the Device and protect the communication from man in the middle / replay attacks.

I.2.2.1.3 Encrypted Device Data Function

This function is used by Device when device is sending any data (like Health Packet or Diagnosis Data or PVT [Position, Velocity, Time] data) to an Application Server.

I.2.2.2 Secure Element Functions

I.2.2.2.1 Decrypt Data Function

This function is called by device and responded by the Secure Element with the result that the Secure Element decrypts the Server Encrypted Data by the use of a key from a specified key index.

I.2.2.2.2 Encrypt Device Data Function

This function is called by device and responded by the Secure Element with the result that the Secure Element encrypts the Device Data by the use of a key from a specified key index.

I.2.2.3 Application Server Functions

I.2.2.3.1 Key Import Function

This function is used by Application Server to import encryption/decryption keys for the SE (Secure Element) from a trusted source. Establishing trusted source is out of scope of this explanation.

I.2.2.3.2 Decrypt Device Data Function

This is function is used by Application Server to request the decryption of incoming data from the device. Application server establishes ‘Identity’ and ‘Authenticity’ of the incoming Device Data request using this function.

I.2.2.3.3 Encrypt Server Data Function

This is function is used by Application Server to request the encryption of data intended to be sent to a device (e.g. a command, like configuration change). When called, this function adds TRUST data which is used by device to establish mutual authentication with the server.

I.2.3 Application Server to Device flow (Sample)

Following is a sample data flow for ‘Command (Remote Management, Configuration Control)’ sent from Application Server to Device.

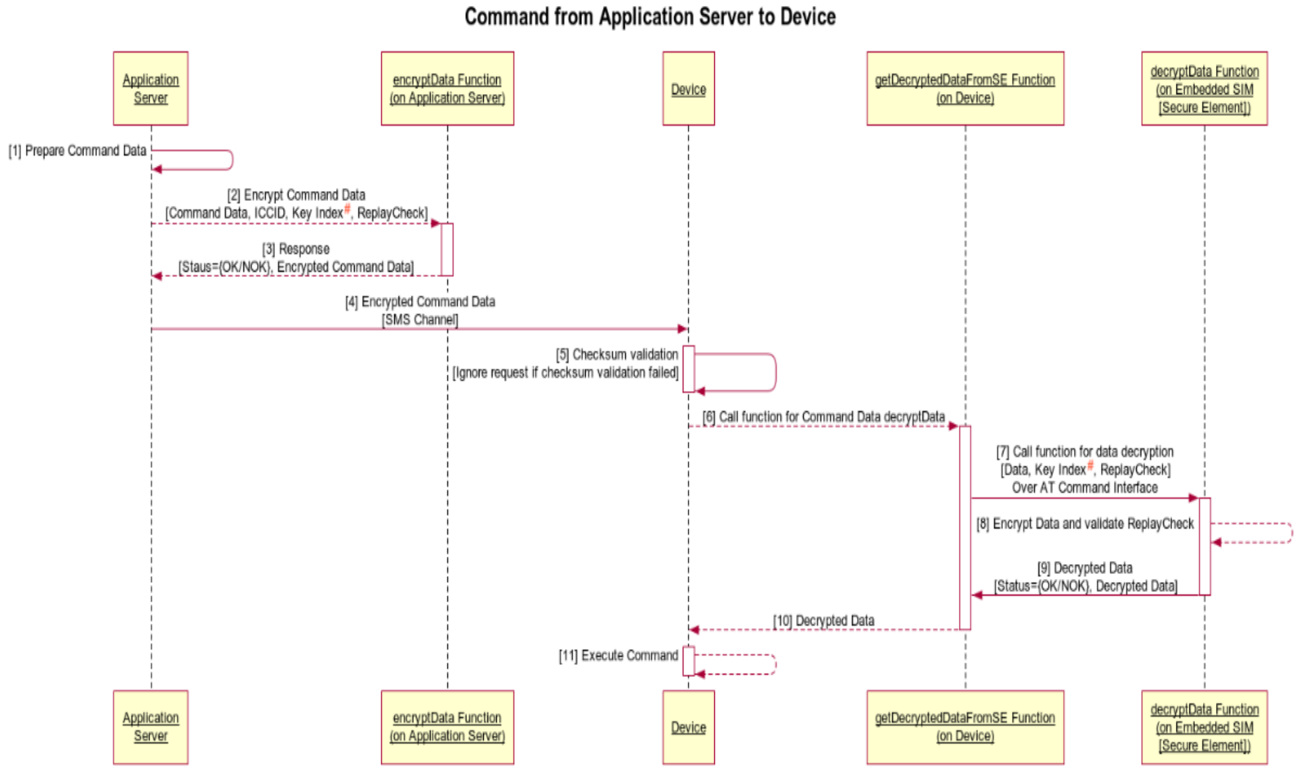

Command from Application Server to Device
Application Server
encryptData Function (on Application Server)
Device
getDecryptedDataFromSE Function (on Device)
decryptData Function (on Embedded SIM [Secure Element])
[1] Prepare Command Data
[2] Encrypt Command Data [Command Data, ICCID, Key Index#, ReplayCheck]
[3] Response [Staus=(OK/NOK), Encrypted Command Data]
[4] Encrypted Command Data [SMS Channel]
[5] Checksum validation [Ignore request if checksum validation failed]
[6] Call function for Command Data decryptData
[7] Call function for data decryption [Data, Key Index#, ReplayCheck] Over AT Command Interface
[8] Encrypt Data and validate ReplayCheck
[9] Decrypted Data [Status=(OK/NOK), Decrypted Data]
[10] Decrypted Data
[11] Execute Command
Application Server
encryptData Function (on Application Server)
Device
getDecryptedDataFromSE Function (on Device)
decryptData Function (on Embedded SIM [Secure Element])

Figure I.2: Application Server to Device Communication Flow

NOTE 1 – # In future, one-time session key, shared using public/private key and crypto challenge could be used instead of fixed keys

Bibliography

[b-RFC 2865] IETF, Request for Comments: 2865 (June 2000), *Remote Authentication Dial In User Service (RADIUS)*

[b-RFC6614] IETF, Request for Comments: 6614 (May 2012), *Transport Layer Security (TLS) Encryption for RADIUS*

[b-RFC7616] IETF, Request for Comments: 7616 (September 2015), *HTTP Digest Access Authentication*.

____