INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG13-TD273/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Geneva, 28 June 2019

TD

Source: Rapporteur

Title: Living list of draft Recommendation ITU-T Y.OBF_trust: "Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems

Purpose: Proposal

Contact: Gyu Myoung Lee
KAIST
Korea (Rep. of)

Tel: +82-42-350-6282
Fax: +82-42-350-6226
E-mail: gmlee@kaist.ac.kr

Keywords: Living list; Open Bootstrap Framework; Q16/13; June 2019

Abstract: This document provides a living list of Q16/13 – "Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems" based on the June 2019 meeting.

This document provides a living list of Q16/13 – Open Bootstrap Framework.

No.	Title of Living Lists	Status
1	Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems	Under Study (June 2019, Geneva)

This document is based on the following contributions.

At the March 2019 Q16/13 meeting.

C-650	India, Ministry of Communications	Providing Trustful access to IoT Devices and Data with a ETSI GBA type Network Authentication Function and Secure Element Services	Q16/13

At the June 2019 Q16/13 meeting.

C-126	India	Open Bootstrap Framework enabling trustful devices, applications and services for distributed diverse ecosystems	Q16/13

1. Introduction:

In its current form, the 3GPP GAA Framework is meant for the Mobile network operators (MNOs) and 3GPP Network elements (e.g. Connected Devices) that use the UICC based SIM/ USIM / ISIM.

A MNO may or may not want to play the role envisaged by the GAA framework. Besides, even if a MNO, as the initial issuer of the subscription, does offer the services of the framework, it is only useful when ALL MNOs offer the framework to allow for seamless changes in subscription during the lifecycle of a connected Device.

With such limitations, 3GPP GAA is not independent of network technology and MNOs.

2. Motivation / Rationale and Scope:

In order to make the framework truly independent, and for the global applicability and usefulness of the GAA, the User / Use Case must be able to benefit from the GAA framework, independent of any one MNO and independent of the Network Technology for connected devices.

The objective of this proposal is to enhance the 3GPP GAA framework to be an Open Bootstrap framework that can be MNO and Network Technology independent to satisfy all present and future trust requirements of devices and network such as enabling federation of Secure Access and Service Control for Devices, Networks, Authentication, Applications and Services across Network Service Providers, M2M Service Providers and Application Providers.

This proposal is an enabler for the harmonisation of a trust framework for ITU, 3GPP and One M2M and non 3GPP networks/ technologies.

In future, proposal may be extended for use of SSC (Support for Subscriber Certificates) mechanism.

3. Proposal

This proposal specifies an Open Bootstrap Framework that can satisfy all present and future trust requirements of devices and network such as enabling federation of Secure Access and Service Control for Devices, Networks, Authentication, Applications and Services across Network Service Providers, M2M Service Providers and Application Providers.

Attachments:

1. **Annexure I** - A.1 Justification for proposed draft new Recommendation Y.OBF_trust
2. **Annexure II** - Draft Recommendation ITU-T Y.OBF_trust "Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems"

Annexure I

A.1 Justification for proposed draft new Recommendation Y.OBF_trust

Question:	16/13	**Proposed new ITU-T Recommendation**	Geneva, Switzerland, 17-28 June 2019	
Reference and title:	ITU-T Y.OBF_trust "Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems"			
Base text:	TD nnnn/WPxx		**Timing:**	2019-JUN
Editor(s):	Abhay Shankar Verma Vijay Kumar Roy Anuj Jain Sharad Arora Jonas Haggard		**Approval process:**	Choose one: AAP | TAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This contribution specifies an Open Bootstrap Framework that allows the Registration, Authentication and Control of Devices (including Constrained Devices), Connected Services & Applications.

In particular, the contribution includes

- An Architecture Reference Model
- An authentication function for the secure element compatible with the functions specified by 3GPP for Universal Integrated Circuit Card based Subscriber Identity Modules that use the 3GPP Generic Bootstrap Architecture
- Four Reference Points for the interaction between secure elements, devices, authentication servers and application servers
- Universal mechanisms for transfer of session keys
- Universal mechanism for digital challenge and response compatible with 3GPP GAA

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

An open Bootstrap Framework is required to provide an umbrella architecture for trustworthy networking of devices, networks, services across network technologies for diverse industry use cases permitting transferability and inter-operability between service providers.

The existing 3GPP Generic Authentication Architecture (GAA), of which Generic Bootstrap Architecture (GBA) is a part, does not support the use of shared secrets in GBA for networks (and the associated devices) which belong to non 3GPP standardization framework.

In order to provide a framework, which can use shared secrets in GBA to diverse use cases and industry verticals, a need has been felt to create a framework for the registration, authentication, authorization and control of applications and services, enabled by the use of frugal, proven, robust and trustful networking elements (e.g. secure elements, authentication functions), which may or may not be based

on 3GPP network technologies. This can be achieved by extending the existing 3GPP GAA and accordingly this recommendation tries to fill the gap, to accommodate non 3GPP networks/ technologies.
Relations to ITU-T Recommendations or to other standards (approved or under development): 3GPP TS 33.220 " Generic Authentication Architecture"
Liaisons with other study groups or with other standards bodies: ITU-T SG17, ITU-T SG20, 3GPP, OneM2M
Supporting members that are committing to contributing actively to the work item: India

Annexure-II

Draft Recommendation ITU-T Y.OBF_trust

Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems

Summary

The objective of this recommendation is to create a framework for the registration, authorisation and control of applications and services, enabled by the use of frugal, proven, robust and trustful networking elements, by extending the 3GPP Generic Authentication Architecture (GAA) framework, to diverse use cases and industry verticals that are dependent on various standards other than 3GPP. This is achieved specifically by extending the mechanism to use shared secrets in Generic Bootstrapping Architecture (GBA) to non 3GPP network technologies. This can benefit the diverse industry verticals that have the need for standardised ICT infrastructure but don't have a standardisation framework like that of the communications industry. The proposal is particularly useful for Constrained Devices (e.g. IoT Devices that use low capability controllers that cannot support crypto functions) as it brings these devices high end security by the use of the secure elements embedded within low cost connectivity elements such as the UICC/ eUICC.

Whilst robust and vendor neutral, the 3GPP Generic Bootstrap Architecture (3GPP GBA), which enables standardisation of authentication and access control across hundreds of Networks, Suppliers and Devices, is not useable generically due to the following limitations

- It is relevant only to 3GPP Networks in Telecoms, usable only by Mobile Network Service Providers
- It does not specify handover and transfers of Service between Networks and Application Platforms

The objective of this contribution is to enhance the 3GPP GAA framework to be an Open Bootstrap framework that can be MNO and Network Technology independent to satisfy all present and future trust requirements of devices and network such as enabling federation of Secure Access and Service Control for Devices, Networks, Authentication, Applications and Services across Network Service Providers, M2M Service Providers and Application Providers.

This contribution specifies a framework for extending the 3GPP GBA/GAA capabilities for design, deployment, and operation of an open authentication framework including authentication functions, reference points, protocols, APDUs and key exchange procedures between Users and Providers of UICC based secure elements, constrained devices, authentication servers and application servers.

Keywords
Trust; Bootstrap; eUICC, Generic Authentication Architecture (GAA), constrained devices, Authentication, Authorisation

Table of Content

Draft Recommendation ITU-T Y.OBF_trust

Open Bootstrap Framework enabling trustworthy networking and services for distributed diverse ecosystems

1. Scope

This contribution specifies an Open Bootstrap Framework that allows the Registration, Authentication and Control of Devices (including Constrained Devices), Connected Services & Applications.

In particular, the contribution includes

- An Architecture Reference Model
- An authentication function for the secure element compatible with the functions specified by 3GPP for Universal Integrated Circuit Card based Subscriber Identity Modules that use the 3GPP Generic Bootstrap Architecture
- Four Reference Points for the interaction between secure elements, devices, authentication servers and application servers
- Universal mechanisms for transfer of session keys
- Universal mechanism for digital challenge and response compatible with 3GPP GAA

2. References

[3GPP TS 33.220 version 15.4.0 Release 15] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)

3. Definitions

3.1 Terms defined elsewhere

This contribution uses the following terms defined elsewhere:

i. **Party**: Natural person or legal person, whether or not incorporated, or a group of either

3.2 Terms defined in this document

This contribution defines the following terms:

i. **Authentication Server:** A Server with the functionality to authenticate a device using one or more authentication protocols.

ii. **Constrained Device**: A device with limitations to process, communicate or store data; limited battery life; limitations to crypto capabilities

iii. **Secure Element:** A tamperproof component of the device that has the capability of store key data and run at least one authentication algorithm.

iv. **Resource Server:** A Server that holds hosts the protected user resources

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

vi. **RPO**: 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.

vii. **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.

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

ix. **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)

x. **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

4. Abbreviations and acronyms

3GPP	The 3rd Generation Partnership Project (3GPP) unites telecommunications standard development organizations (ARIB, ATIS, CCSA, 3GPP, TSDSI, TTA, TTC)
BSF	Bootstrapping Server Function
eUICC	Embedded UICC, a UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the Device, and enables the secure changing of Profiles over the air
EID	eUICC-ID
HLR	Home Location Register
IoT	Internet of Things
M2M	Machine to Machine
MNO	Mobile Network Operator
NAF	Network Application Function
OBF	Open Bootstrap Framework
OneM2M	is a global organization that creates requirements, architecture, API specifications, security solutions and interoperability for Machine-to-Machine and IoT technologies
SIM	Subscriber Identification Module, a secure element containing subscription identifier in a 3GPP network
SLF	Subscriber Locator Function
TSP	Telecom Service Provider, see also MNO
UE	User Equipment – Typically a mobile phone with a SIM or UICC
UICC	Universal Integrated Circuit Card, a newer version of the SIM

5. Conventions

Nil

6. Overall structure of Open Bootstrap Framework

6.1. Concept of Open Bootstrap Framework

The emergence of new technologies including Internet of Things and Machine to Machine Communications is changing the world in each and every dimension. The connected device space is growing rapidly, adding a wide variety of disparate devices, application and services in the market. This growth comes with many challenges in terms of Identification, Authentication, Authorisation and Data Integrity. To orderly enable large scale deployment, there is need for an open bootstrap framework to fill the gap created due to expected increase in various types of connected devices of existing and forthcoming technologies.

The 3GPP Generic Authentication Architecture is a proven framework, which have not been compromised over a 30-year period, for identifying and authenticating a device where an Authentication Server and the Secure Element shall mutually authenticate and agree on session keys that are afterwards applied between Secure Element and an Application Server. The Authentication Server shall restrict the applicability of the key material to a specific Application Server depending on the rights set is the Resource Server. The lifetime of the key material is set according to the local policy of the Authentication Server

The Figure below reproduces the 3GPP Generic Authentication Architecture Reference Model as per [3GPP TS 33.220] showing a simple network model for bootstrapping.

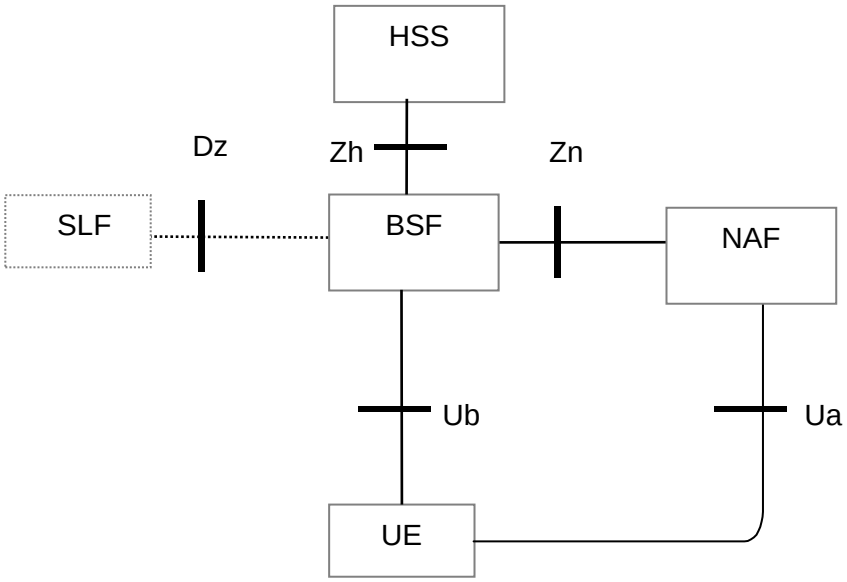

Figure 1: 3GPP GAA Reference Model

In its current form, the 3GPP GAA Framework is meant for the Mobile network operators (MNO) and 3GPP Network Connected Devices that use the UICC based SIM / USIM / ISIM.

A MNO may or may not want to play the role envisaged by the GAA framework. Besides, even if a MNO, as the initial issuer of the subscription, does offer the services of the framework, it is only useful when ALL MNOs offer the framework to allow for seamless changes in subscription during the lifecycle of a connected Device.

In addition, the GAA must become network technology independent i.e. it must accept that connected Devices will use non-3GPP Technologies in the times to come. For the global applicability and usefulness of the GAA, the User / Use Case must be able to benefit from the GAA framework, independent of any one MNO and Network Technologies.

The objective of the concept described below is to enhance the 3GPP GAA to be an Open Bootstrap framework that can be MNO and Network Technology independent. The Requirements, Architectures and Mechanisms are proposed in the sections below.

High Level Concept Diagram:

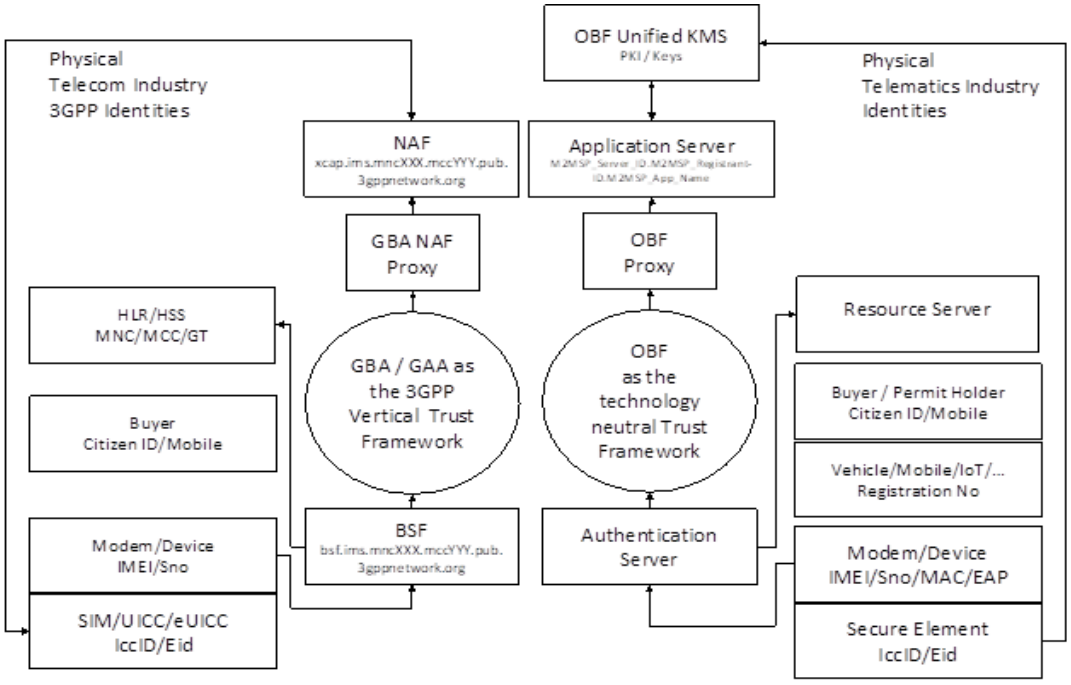

Figure 2. 3GPP and Open Bootstrap Framework Concept

6.2. Requirements

a) The OBF is required to be independent of MNO, M2M Service Provider (M2MSP) and Application Service Provider (ASP), permitting users to freely move between MNOs, M2MSPs and ASPs.

b) The OBF is required to be Network technology agnostic, supporting the 3GPP connected devices as per the 3GPP GAA framework as well as other devices due to M2MSP/IoT deployment.

c) Since users may change MNOs/M2MSPs frequently over their lifetime, whilst they may remain loyal to the many applications, it is required that the users and devices shall be able to utilize the Authentication service from a new MNO/M2MSP as per the process defined in this contribution

d) There is a requirement for a process to transfer key data to a new MNO/M2MSP/ASP.

e) The M2MSP/ASP is required to be allowed to play the role of the provider of the Authentication Services, in addition to the MNO

f) With the large proliferation of the Embedded SIM, the physical SIM is no longer the property of a single MNO. Subscriptions can be changed over the air, without changing the physical card. It is required that the device shall be able to forward the authentication requests to the new Authentication Server in case of changes in subscription of MNOs, M2MSPs, and ASPs in order to accommodate SIM viz. remote provisioning.

g) Most importantly, in the new IoT Applications domain, a single device may have several beneficiaries in the ecosystem. This fact is illustrated by the picture below, which shows the potential beneficiaries of the Data generated from a single Telematics device in a Public Transport Vehicle:

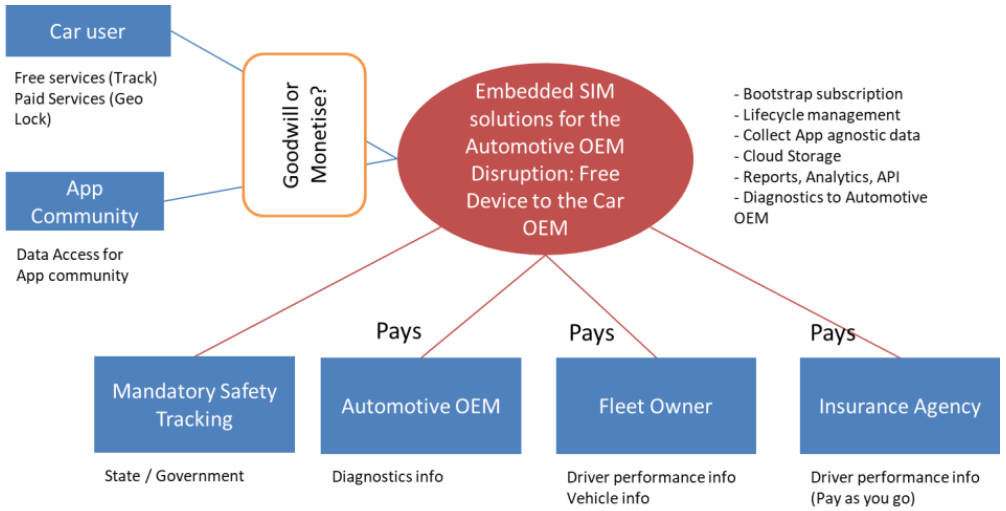

Figure 3. Multiple applications accessing single device

The OBF is required to permit multiple beneficiaries to have control over the security of a limited part of the data generated from the device. For example, the state may want that the alarms initiated from the device to be encrypted and sent only to the National Emergency Response System. This nature of disaggregated control of authentication and encryption is not possible within the current framework.

h) The OBF enables Applications outside the MNO domain to use the framework to authenticate devices and access data.

i) The OBF enables multiple beneficiaries of an IoT Device/IoT Device Data to simultaneously benefit from the security framework without compromising/interfering with the privacy/security requirements of the other beneficiary.

6.3. Capabilities of Open Bootstrap Framework

The capabilities of the Open Bootstrap Framework are proposed as follows:

a) Capability for registration of MNOs, M2MSPs, and ASPs

b) Capability for registration of USIM/ISIM/Secure Elements and the Connected Devices in which the USIM/ISIM/Secure Element is embedded

c) Capability for import and exchange of Keys for the authentication of Connected Devices by the Applications that provide access to the Connected Devices

d) Capability of transfer of Connected Devices between MNOs, M2MSPs, and ASPs

e) Capability to remain agnostic of the Network Technology whilst remaining compatible with the 3GPP GAA

7. Architecture

7.1. Reference Model

The proposed Open Bootstrap Architecture Reference Model is shown below:

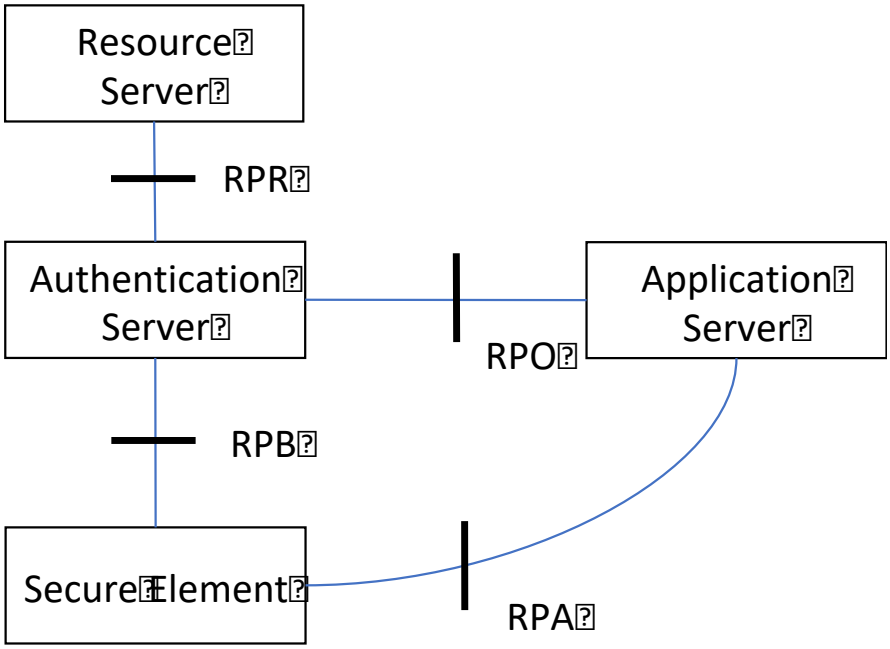

Figure 4 Open Bootstrap Architecture Reference Model

7.2. Functional Model

The Functional Model of the Open Bootstrap Framework showing backward compatibility with the 3GPP GAA is shown below. The OBF enables a MNO/M2MSP/ASP to benefit from trusted third-party frameworks for the transfer of the user and the user device

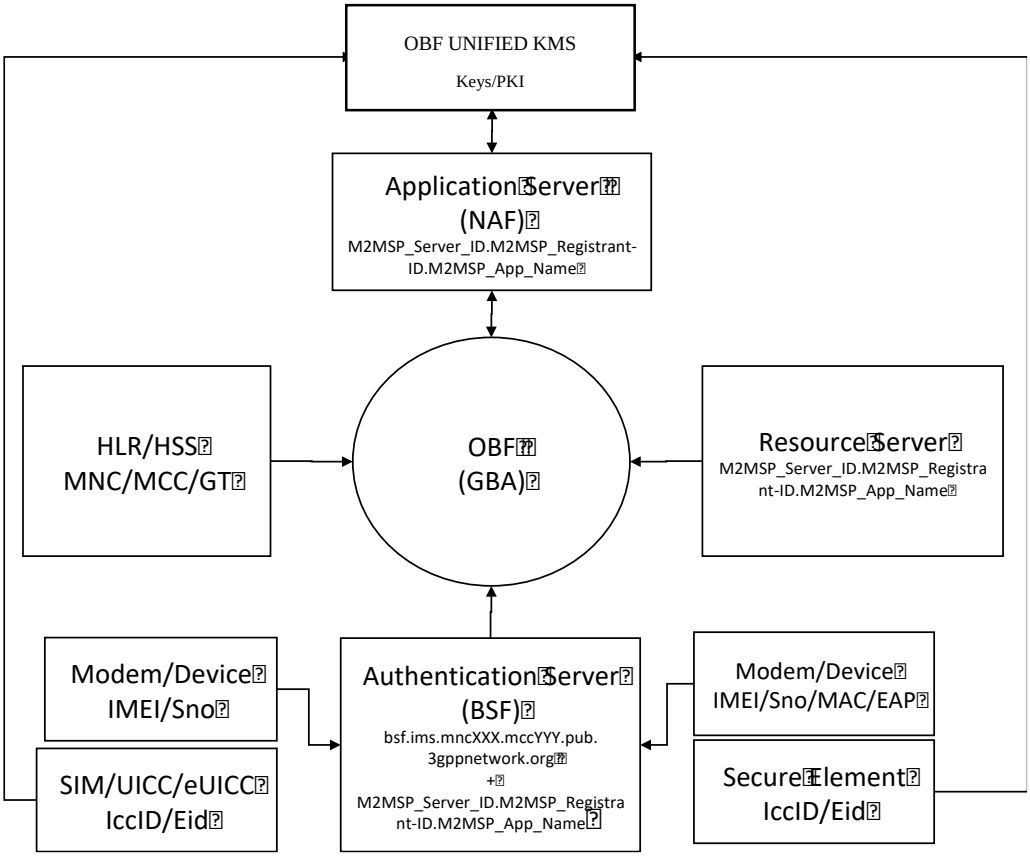

Figure 5. Functional Model of the Open Bootstrap Framework

7.3. Reference Points

The following Reference Points are proposed as per the Figure 4 Open Bootstrap Architecture Reference Model.

RPR: The Reference Point between Authentication Server and Resource Server. Here the Authentication Server can get the resource rights for a certain device.

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.

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.

RPA: The Reference Point is between Secure Element and Application Server. It carries the application protocol, which is secured using the keys material agreed between Secure Element and Authentication Server

7.4. Functions

Authentication Functions implemented in the Secure Element, Device and the Servers which are involved in the Authentication process are as proposed below:

The Authentication Function is hosted in the network of the MNO/M2MSP/ASP under the control of the issuer of the card (any of SIM/USIM/ISIM/Smart card). The Authentication Server, Resource Server, and Secure Element participate in the Generic Authentication Architecture in which a shared secret is established between the network (Authentication Server) and a Secure Element by running the bootstrapping procedure over the reference point

RPB (which may be the Ub interface if the Device is 3GPP Network Connected). The shared secret can be used between Application Servers and the Secure Element, for example, for authentication purposes, after an application server has received the corresponding key material over the reference point RPO (which may be the Zn interface if the Device is 3GPP Network Connected).

Secure Element Function - Bootstrap:

A function of the Secure Element that executes the bootstrapping procedure with Authentication Server and provides the ME / Device applications with security association to run bootstrapping usage procedure.

Secure Element Function - Application:

An Application Server calls this function over the reference point RPA (which may be the Zn interface if the Device is 3GPP Network Connected) when an application server wants to use bootstrapped security association.

7.5. Mechanisms

The contribution proposes the following mechanisms to realise the requirements:

a) A Mechanism for **mutual Authentication** between the Secure Element and Authentication Server over RPB such that there can be no doubt from either side they are communicating with the trusted party.

b) Defines the process for **changing Authentication Servers**, in cases where device may be shipped across the world and the current Authentication service is no longer available. The Public/Private keys shall facilitate such a transfer by storing the Authentication Server Public Key (B) in the Secure Element after validating it using Authentication Server A Public key (sign)

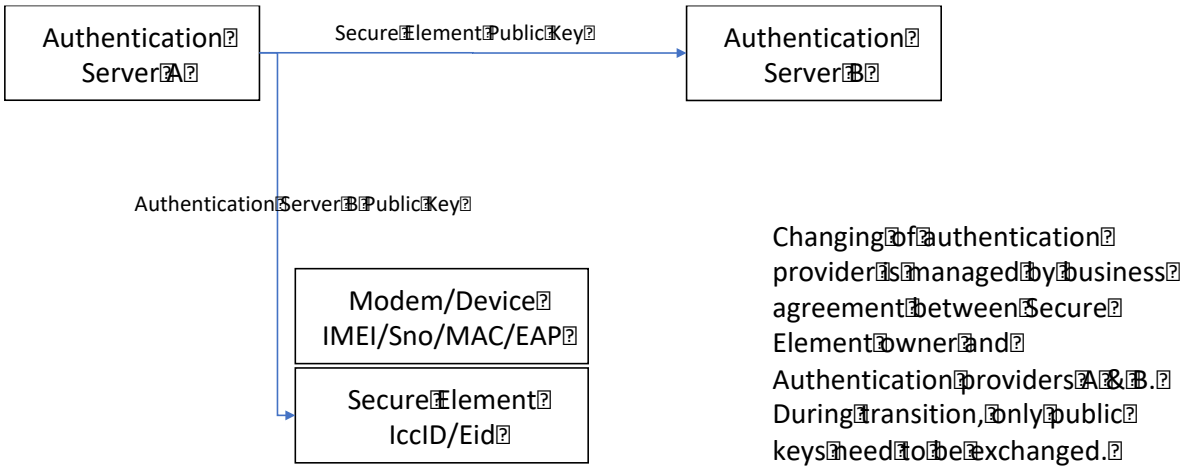

Figure 6. Transfer of Authentication Service Provider

Note: The Mechanism for device authentication towards the Applications / Applications Servers on behalf of the device (Know-Your-Customer norms for verification of a trusted Device / User) shall remain as per the accepted norms of Diameter protocol / User Access Management and is not in the scope of this submission.

8. High-level Procedures for the OBF

8.1. Bootstrapping Process

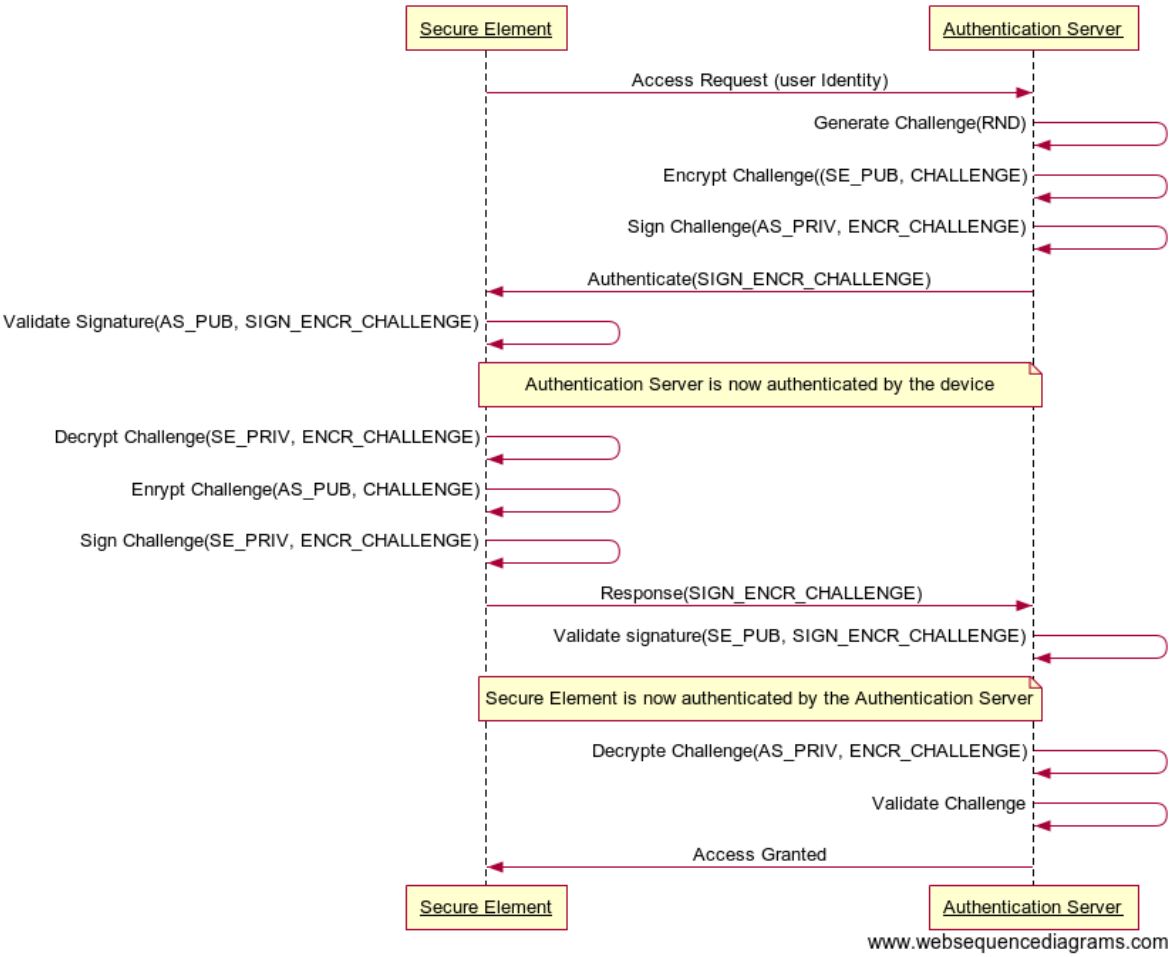

Figure 7. Bootstrap procedure

8.2. Authentication Server Change Process

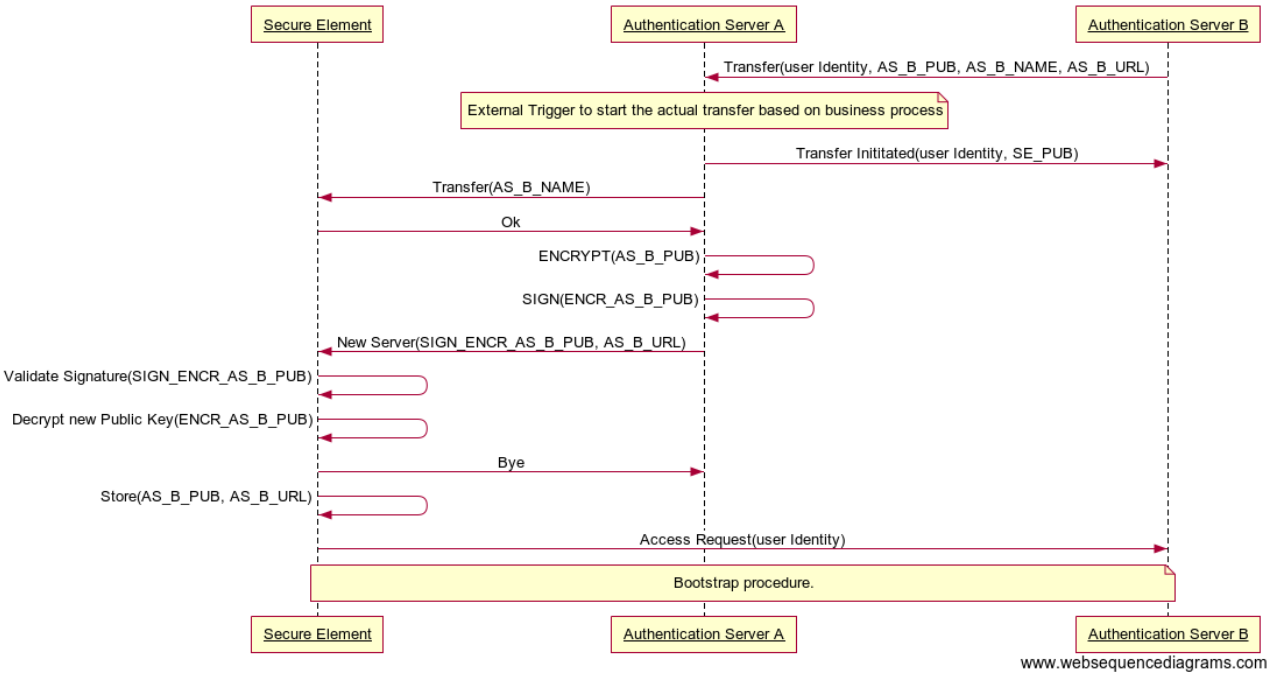

Figure 8. Authentication Server Change

Bibliography

[F.748.1] SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES, *Requirements and common characteristics of the IoT identifier for the IoT service*.

[Y.4500.13/Q.3954] Testing specifications – Testing specifications for next generation networks, *oneM2M – Interoperability testing*.

[b-TRAI] Recommendations on Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications, Telecom regulatory Authority of India, 5 Sep2017

[b-GSMA] GSMA: "GSMA IoT Security Guidelines and Assessment"

https://www.gsma.com/iot/iot-security/iot-security-guidelines/.

[TEC-TR-SN-M2M-009-01] Technical Report, *Recommendations for IoT / M2M Security*

[b-NIST] NIST Special Publication 800-63B: "Digital Identity Guidelines - Authentication and Lifecycle Management" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

Appendix – I: Real-world explanation of the use case example

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

1.1 Background

The use case (see clause 1.2) is a real-world use case in India. 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 must have mechanisms to establish the Integrity, Identity, Authenticity and Trust to ensure the secure and trustful implementation of public safety for the citizens.

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

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 must be able to identify the device correctly
2. Application server must be able to check the data integrity which means no one in between have changed the data
3. Application server must 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 must be able to identify that this request is coming from authorized application server
2. Device must be able to check the data integrity which means no one in between have changed the data
3. Device must be 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

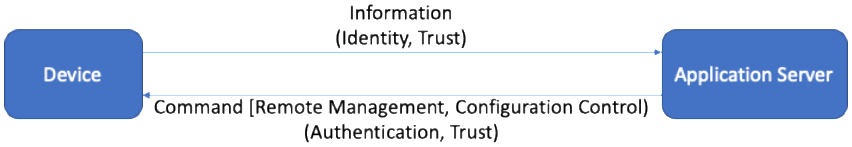

*Figure A.**1**: Device-Application Server Communication*

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.

2.2 Functions required

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

2.2.1 Device Functions

2.2.1.1 Validate Checksum Function

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

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 shall 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.

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.

2.2.2 Secure Element Functions

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.

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.

2.2.3 Application Server Functions

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.

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.

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.

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.

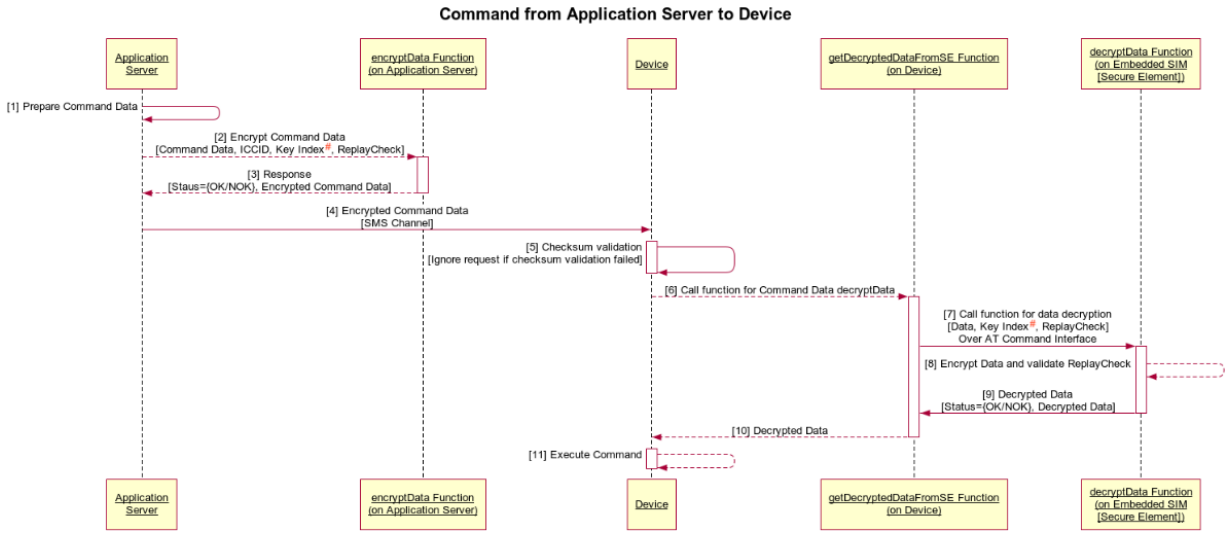

Figure A.2: Application Server to Device Communication Flow

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

3 Conclusions

In the example cited above, the use case belongs to the domain of Public Transport. The connected Machines are public service vehicles. The affected industry is either the Automotive industry and/or the Embedded Electronics industry.

The Ecosystem comprises of tens of Automotive Companies, hundreds of VTS Device Manufacturers, many MNOs, SIM Providers and Application Service Providers. Vehicles registered in one state will move freely into other states. However, the use of the secure element embedded in the UICC unifies the mechanism of secure registration, certification, Machine Know-Your-Customer (KYC), Secure Device Management etc. for the entire ecosystem. The Secure Element embedded in the SIM card provides the root of trust. Every VTS device may not have controllers that support crypto functions. Yet, the crypto libraries of the 3GPP SIM can be used to establish a trustful session with the Tracking and Alarms Management Servers.

The example illustrates how

- Diverse industries, with a large number of stakeholders and multitude of providers, can benefit from the security inherent in the Secure Element of the SIM
- The registration, authentication and control of public transport services is managed by establishing a trustful framework based on the capabilities of the network infrastructure
- Vehicle owners / Devices can move freely from one Network to another using the capabilities of the remote provisionable SIM