INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG13-TD236/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Victoria Falls, 4 – 14 March 2019

TD

Source: Rapporteur

Title: Living list: Open Bootstrap Framework enabling trustful devices, applications 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: Trust; Bootstrap; Authentication

Abstract: This document provides a living list of Q16/13 – Open Bootstrap Framework enabling trustful devices, applications and services for distributed diverse ecosystems.

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

No.	Title of Living Lists	Status
1	Open Bootstrap Framework enabling trustful devices, applications and services for distributed diverse ecosystems	Under Study (March 2019, Victoria Falls)

This document is based on the following contribution.

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

Background:

The Communications and other Industry verticals use ICT services at a mammoth scale today. In order to avoid creation of silos, isolated players and solutions that create a very fragmented market, all emerging industry verticals need to have a fundamental Standardization approach like that prevailing in the Communications industry.

Standards are required to create an open marketplace for sharing data, enabling the creation and discovery of new data-driven Intelligent services, without compromising the security and privacy of the users and the data. This necessarily requires a neutral, national (and international) level framework that supports a federated approach to data platforms, which allows organizations of all types (Public and Private, Telephony and non-telephony) and its customers to use a technology and supplier neutral future-proof digital infrastructure, enabling a wide ecosystem of vendors and platforms to share datasets and data-driven solutions, ensuring inter-operability and transferability to prevent vendor lock-in. This requires the federation of platforms from multiple vendors, ensuring that authentication, access control and service control can be exerted from a cost-efficient, scalable and future-proof digital infrastructure.

The ETSI specified Generic Bootstrap Architecture (ETSI GBA) is one such framework, which enables standardisation of authentication and access control across hundreds of Networks, Suppliers and Devices. Whilst robust and vendor neutral, the ETSI GBA suffers from some deficiencies, viz.

- It is relevant only to 3GPP Networks in Telecoms
- The specification is such that it can only be used by Mobile Network Service Providers
- It does not specify handover and transfers of Service between Networks and Application Platforms
- Non-specific to the Communications industry, for use in any Industry Vertical, yet benefitting from the use of the trusted network infrastructure
- Frugal and cost-effective realisation of the security capabilities for ubiquitously presenting, delegating and controlling the security of devices and applications
- Application and Service Neutral, enabling federation of Secure Access and Service Control for Devices, Networks, Applications and Services across Network Service Providers, M2M Service Providers and Application Providers
- Ensures a common visibility, transferability and inter-operability of Authentication and Service Control across Users / Buyers, Network Service Providers, M2M Service Providers and Application Service Providers
- Define functions to support National Trust Centres / Accreditation labs / Certifying Bodies in deploying trusted ICT infrastructure

Attachments:

Living List - “Open Bootstrap Framework enabling trustful devices, applications and services for distributed diverse ecosystems”

Appendix – I: Use Case Example

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

Summary

The objective of this draft Recommendation is to contribute a framework for the registration, authorisation and control of applications and services, enabled by the use of frugal, proven, robust and trustful networking elements, extending the ETSI Generic Bootstrap Architecture, to diverse use cases and industries, that can benefit from 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 Draft Recommendation 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 ETSI Generic Bootstrap Architecture (ETSI 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 Recommendation is to specify a framework for extending the ETSI GBA 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; Authentication

Table of Content

1. Scope

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

In particular, the recommendation includes

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

2. References

[ETSI TS 133 220] Technical Specification ETSI, v6.4.0 2005, Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220 version 6.4.0 Release 6)

3. Definitions

3.1 Terms defined elsewhere

This Recommendation 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 Recommendation 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, ETSI, 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
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. Overview of Open Bootstrap Framework

6.1. Overall Concept

The development of the Internet of Things and Machine to Machine Communications is changing the world in each and every dimension. Most of the existing M2M solutions are vertical/industry specific applications. This could affect the development of large-scale deployments. The M2M device space is growing rapidly, adding a wide variety of disparate devices in the market. This growth comes with many challenges in terms of Identification and Data Integrity.

The ETSI 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 shows a generic Bootstrap Architecture as per [ETSI TS 133 220]

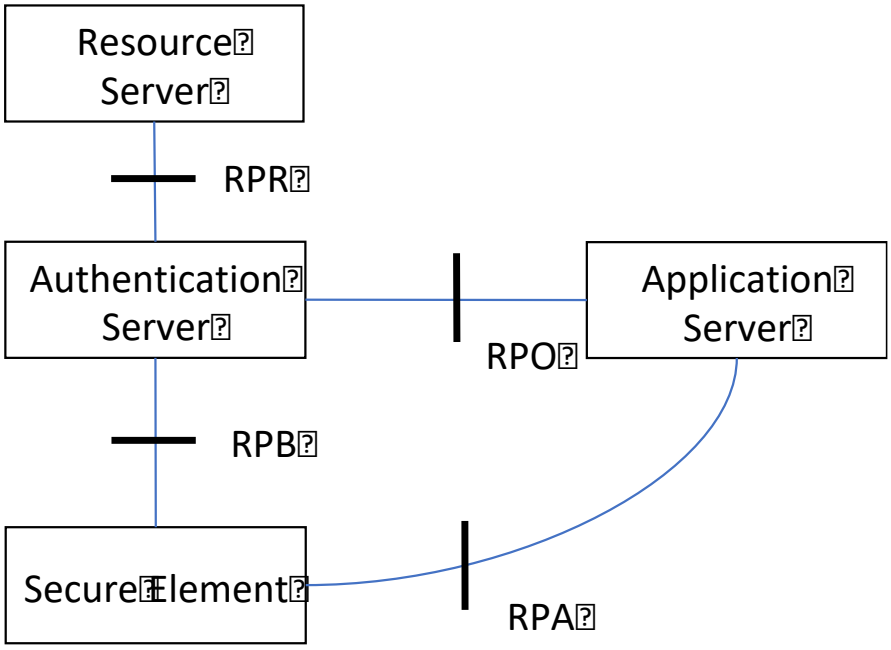

Figure 1: Generic Bootstrapping for Access Control

In the framework cited above, the following basic functions and capabilities are identified.

Authentication Server Function:

The Authentication is hosted in the network under the control of an Mobile Network Operator (MNO). 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. 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.

Secure Element Function:

A function on the Secure Element executing the bootstrapping procedure with Authentication Server and providing Ua applications with security association to run bootstrapping usage procedure. An Application Server calls this function over the reference point RPA when an application server wants to use bootstrapped security association.

The shortcomings of the ETSI GBA are proposed to be corrected by the Requirements, Architectures and Mechanisms proposed in the sections below. In its current form, the ETSI GAA Framework is Telecom Service Provider (TSP). A TSP may or may not want to play the role. In which case, the User / Use Case cannot benefit from the framework.

High Level Concept Diagram:

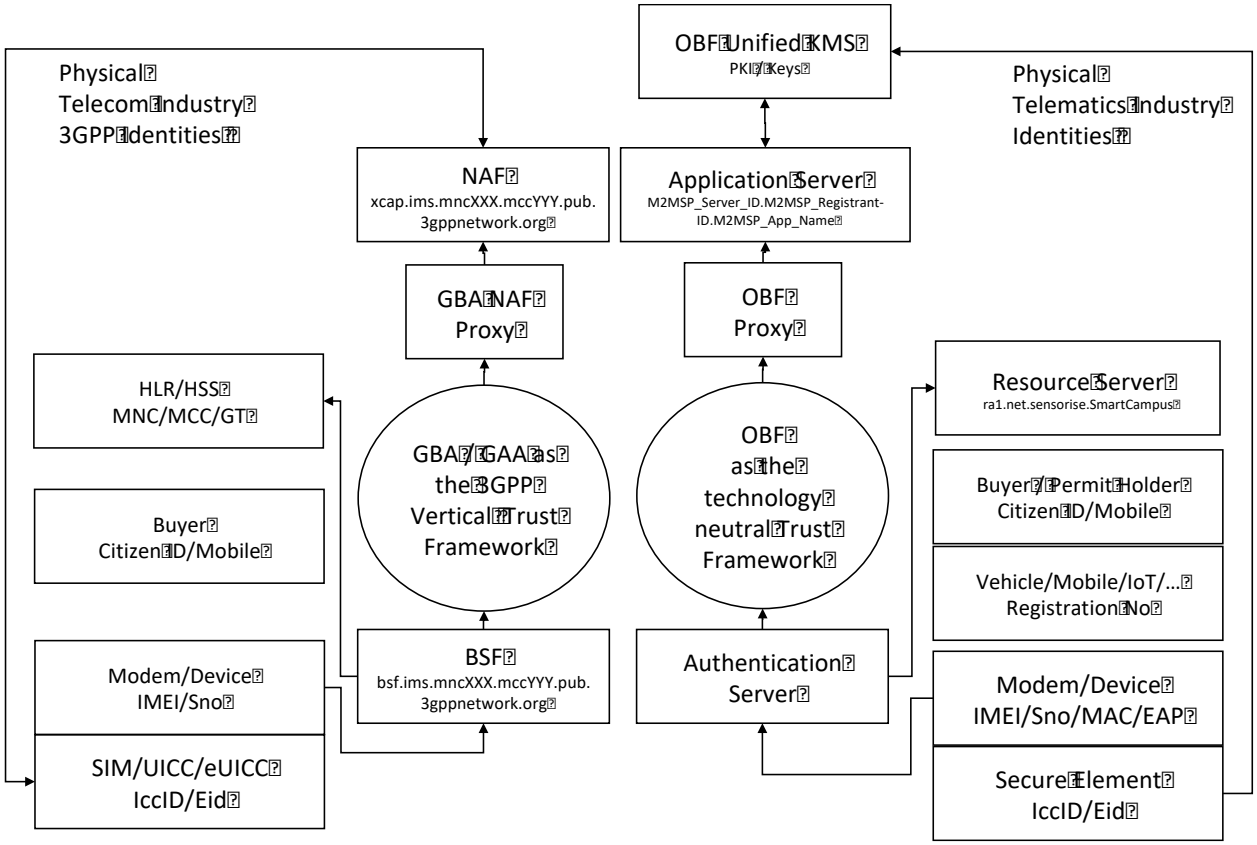

Figure 2. ETSI and Open Bootstrap Framework Concept

6.2. Architecture

The incorporation of the ETSI GBA Architecture for the Open Bootstrap Architecture is shown below. The OBF enables a TSP/M2MSP/ASP to benefit from trusted third party frameworks for the transfer of the user and the user device

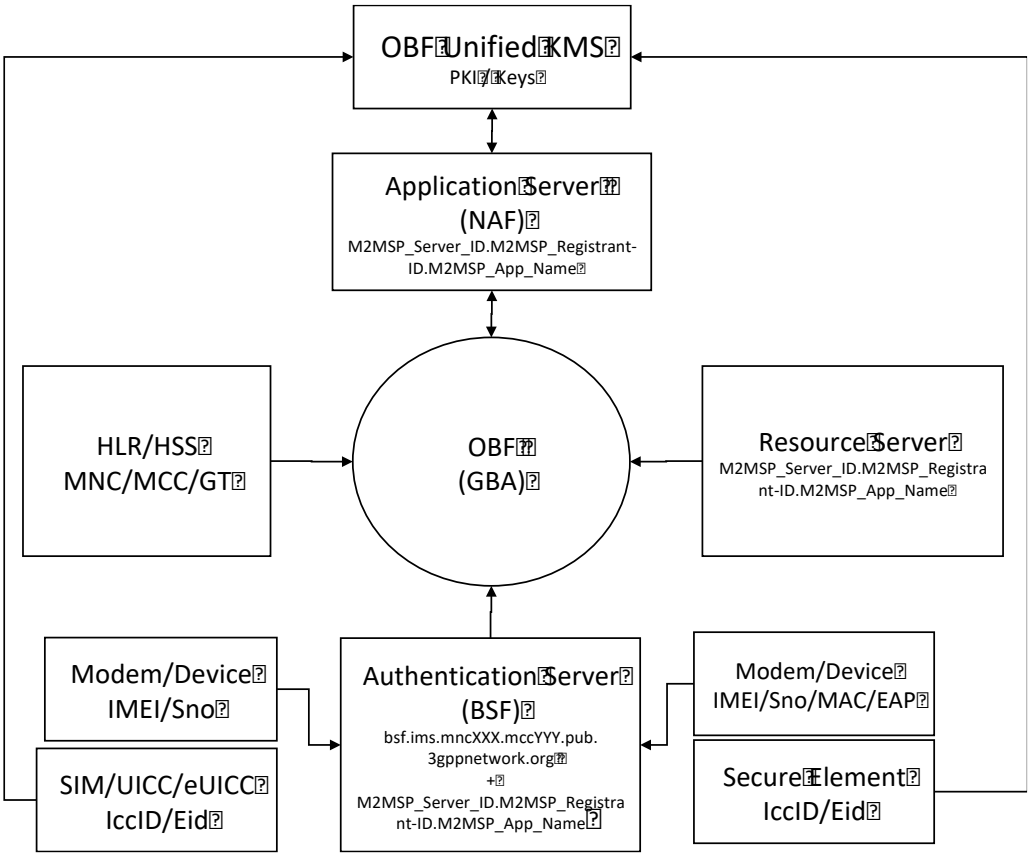

Figure 3. Concept of the Open Bootstrap Framework

6.3. Requirements

6.3.1. Requirement Definition

a) The OBF is required to be Telecommunications Service Provider (TSP), M2M Service Provider (M2MSP) and Application Service Provider (ASP) neutral, permitting users to freely move between TSPs, M2MSPs and ASPs.

b) Since users change TSPs/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 TSP/M2MSP as per the process defined in this recommendation

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

d) The M2M SP / ASP is required to be allowed to play the role of the provider of the Authentication Services, in addition to the TSP

e) With the large proliferation of the Embedded SIM, the physical SIM is no longer the property of a single TSP. Subscriptions can be changed over the air, without changing the physical card. The recommendation requires that to benefit from the new attribute of the remote provisionable Embedded SIM, M2MSPs and ASPs shall be forwarded the new Authentication Server if the subscription changes

f) 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:

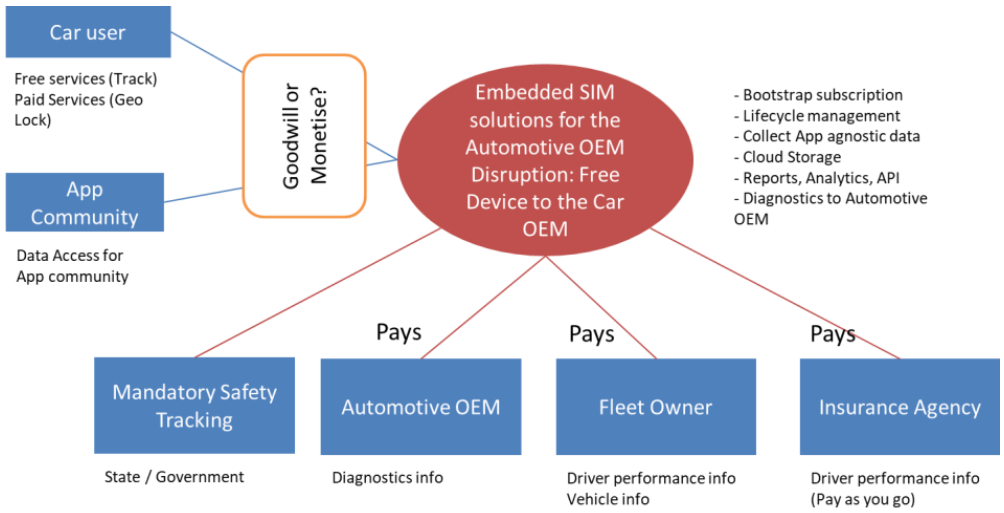

Figure 4. Multiple applications accessing single device

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

g) The OBF enables Applications outside the TSP domain to use the framework to authenticate devices and access data

h) The OBF enables permits 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

6.4. Capabilities of the recommended framework

6.4.1. Authentication Functions

Authentication Functions are implemented in the Secure Element, Device and the Servers involved in the Authentication

6.4.2. Reference Points

The following Reference Points are defined

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

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.

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 carries the application protocol, which is secured using the keys material agreed between Secure Element and Authentication Server

6.4.3. Mechanisms

The draft Recommendation proposes the following mechanisms to realise the requirements:

a) Defines the process for switching Authentication Server, in cases where device may be shipped across the world and the current Authentication service is not 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)

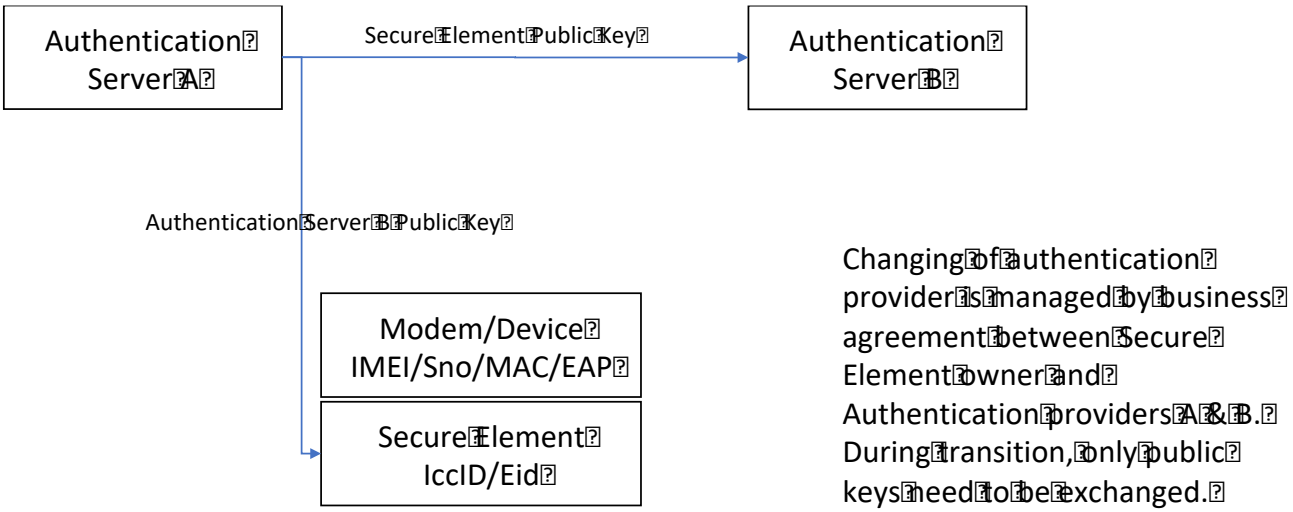

Figure 5. Transfer of Authentication Service Provider

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

B.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 provider 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

B.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.

B.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 AIS140standard 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 TSP (Telcom Service Provider) 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

B.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

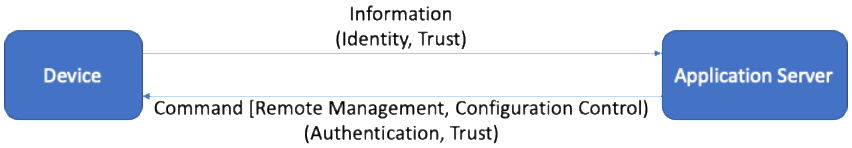

Figure B.6: Device-Application Server Communication

B.2.1 Important consideration for security

Following are important consideration for security implementation:

1. ICCID of embedded SIM (SE) is used as identity of the device/field node
2. Security key is being used trust factor (Asymmetric key infra could be used in future)
3. Security key of the SE is available to SE and Application Server (via key import function) both. In a public/private key infra, public key of other party will be available to each party.

B.2.2 Functions required

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

B.2.2.1 Device Functions

B.2.2.1.1 validateChecksum 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.

Function: validateChecksum	
Input	Checksum Input Data

Response	Checksum

TABLE B.1 – validateChecksum Function Input Output

B.2.2.1.2 getDecryptedDataFromSE Function

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

Device will use 'getDecryptedDataFromSE' function to pass the data to SE, over AT commands, for decryption of data. Along with Encrypted data, this function also adds few more information, like key index, before sending to SE.

Function: getDecryptedDataFromSE	
Input	Encrypted Data
Response	Deciphered Data

TABLE B.2 – getDecryptedDataFromSE Function Input Output

If deciphered data received as response to 'getDecryptedDataFromSE' function call is correct then It establish following facts for device:

1. **Authenticity**: Data is coming from authenticated source
2. **Trust /No Replay Attack**: Since SE also validates the counters ("see clause B.2.2.2.1") after deciphering the incoming data (which may be a command to change configuration of device) and respond deciphered data only when counter check is validated, Device establishes TRUST and executes the command

B.2.2.1.3 getEncryptedDataFromSE 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 Application Server.

When this function is called, device sends input data to SE over AT interface.

Function: getEncryptedDataFromSE	
Input	Data to Send towards Application Server
Response	Ciphered Data

TABLE B.3 – getEncryptedDataFromSE Function Input Output

NOTE 1 – "see clause B.2.2.2.2" for details.

B.2.2.2 Secure Element Functions

B.2.2.2.1 seDecryptData Function

This function is called by device's 'getDecryptedDataFromSE' function and when called, it does following:

1. Receive encrypted data from device over AT interface
2. Decrypt the data using the given key index
3. If ReplayCheck is requested then validate the received data for Replay Check to ensure TRUST
4. If ReplayCheck is requested and found NOK then send the empty response to function call otherwise send the decrypted data as response to function call
5. If ReplayCheck is not requested then send the decrypted data as response to function call

Function: seDecryptData	
Input	Encrypted Data, Key Index, ReplayCheck
Response	Deciphered Data

TABLE B.4 – seDecryptData Function Input Output

NOTE 1 – SE will maintain separate keyset for decryption and encryption function which means key at key index 1 for encryption will different than key at key index 1 for decryption.

NOTE 2 – In future, one-time session key, shared using public/private key and crypto challenge could be used instead of fix keys

B.2.2.2.2 seEncryptData Function

This function is called by device's 'getEncryptedDataFromSE' function and when called, it does following:

1. Receive data to be encrypted from device over AT interface
2. If ReplayCheck is requested then add TRUST data to the input data
3. Encrypt complete data with the requested key
4. Send the encrypted data as response to function call

Function: seEncryptData	
Input	PlainText Data, Key Index, ReplayCheck
Response	Ciphered Data

TABLE B.5 – seEncryptData Function Input Output

NOTE 1 – SE will maintain separate keyset for decryption and encryption function which means key at key index 1 for encryption will different than key at key index 1 for decryption.

NOTE 2 – In future, one-time session key, shared using public/private key and crypto challenge could be used instead of fix keys

B.2.2.3 Application Server Functions

B.2.2.3.1 importKey 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.

Function: importKey	
Input	ICCID, Key, Key Index, Key Function (Encrypt/Decrypt)
Response	Import Status (OK/NOK)

TABLE B.6 – importKey Function Input Output

B.2.2.3.2 decryptData Function

This is function is used by Application Server to request the decryption of incoming data from the device.

Function: decryptData	
Input	Encrypted Data, ICCID, Key Index
Response	Decrypted Data

TABLE B.7 – decryptData Function Input Output

When called, this function retrieves the decryption key at key index for requested ICCID and decrypts the Encrypted Data and send the decrypted data as response to function call. If no decryption key is found for the requested key index and ICCID, function sends an empty response.

Application Server calls this function after receiving a request from the device. If Application Sever gets decrypted data to the 'decryptData' function call, Application server establishes 'Identity' and 'Authenticity' of the request. Once Identity and Authenticity is established, Application Server process the request.

B.2.2.3.3 encryptData Function

This is function is used by Application Server to request the encryption of command, like configuration change, which Application Server is sending to the device.

Function: encryptData	
Input	Command Data, ICCID, Key Index, ReplayCheck
Response	Encrypted Data

TABLE B.8 – encryptData Function Input Output

When called, this function retrieves the encryption key at key index for requested ICCID and encrypts the Command Data and send the encrypted data as response to function call. If 'ReplayCheck' is request in call then this function also adds TRUST data which is used by device to establish the TRUST.

B.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.

B.2.3.1 Data Packet Format

B.2.3.1.1 Command Sent

Example change IP 1 address:

Command:
#ip1 127.0.0.1 8080

Hex Converted:
23697031203132372e302e302e312038303830

B.2.3.1.2 Complete Message

Complete enveloped message which will be received on the device:

027000002811010015FFFFFFFF00000000000368e70c3223697031203132372e302e302e312038303830000000

B.2.3.1.3 Detail of Received Message

027000 -> Indicates its command data from Application Server -> 03 octet

00281101001515A00003
^^^^ -> 0x00 0x28: Data Packet Length -> 40 octet
^^ -> 0x11: Header Length -> 17 octet
^^^^ -> 0x01 0x00: Checksum, Encryption and ReplayCheck Identifier-> 02 octet
^^ -> 0x15: Key Index Identifier -> 01 octet
^^ -> 0xFF: RFU
^^^^^^ -> 0xFFFFFF: Application Reference Number (RFU)

00000000000368e70c32
^^^^^^^^^^ -> 0000000000: 5 octets of CNTR to be used in ReplayCheck
^^ -> 0x03: 1 octet of PCNTR (padding counter length)
^^^^^^^^ -> 68e70c32: 4 octets of Redundancy Check

And the remainder is the command payload with some padding bytes at the end:
23697031203132372e302e302e312038303830000000

B.2.3.2 Flow

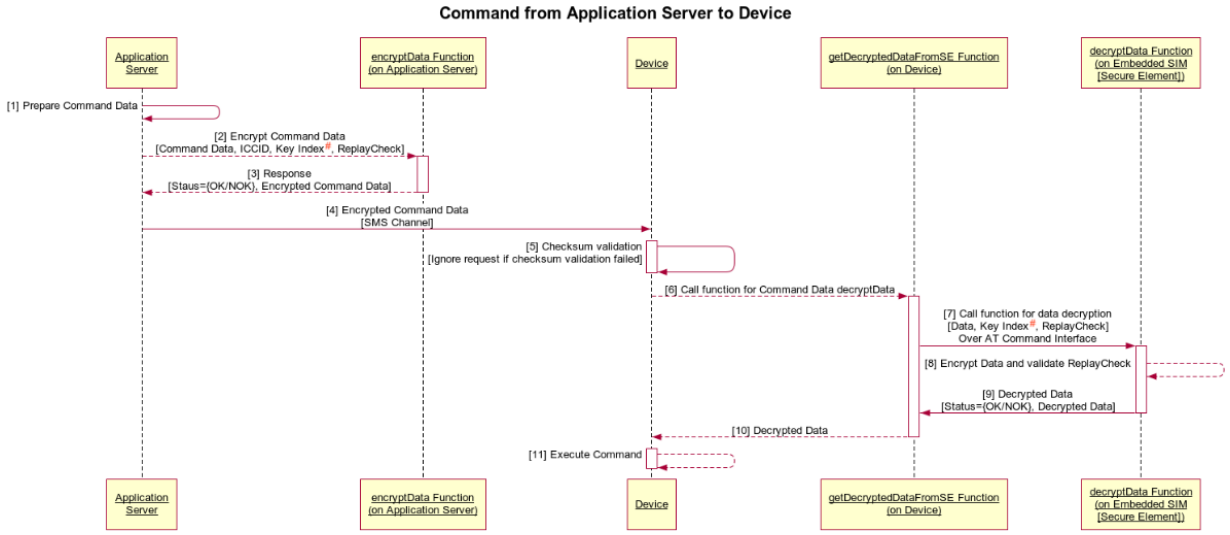

Figure B.7: Application Server to Device Communication Flow

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

B.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. More than 30 States will independently implement the Tracking and Alarms Management Servers. 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 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

_____