Internet of Things

Solutions to Enhance IoT Authentication Using SIM Cards (UICC)

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to explain how authentication can be enhanced within present day and future IoT services by leveraging a UICC (or SIM card) based technology.

SIM cards are used by Mobile Network Operators (MNOs) to authenticate a device (or user equipment) accessing their network and services. In addition to this core function, SIM cards can support additional security capabilities that can be used by IoT service providers, in coordination with their MNO partners, to enhance the security of IoT services.

This document will describe several methods that leverage the security features supported within SIM cards to enhance the authentication of IoT devices within IoT services.

The use of the term "SIM Card" within this document is used to describe a UICC (as defined by ETSI [5] [10]) that may or may not be remotely provisionable (as per the GSMA eUICC Remote Provisioning Architecture specifications for machine-to-machine [18] and consumer devices [19]).

1.2 Scope

The scope of this document is limited to:

- **The use of SIM Card security solutions that are based upon standardised technologies, noting that such technologies, whilst standardised, may not presently be commercially deployed.**
- **The enhancement of authentication within IoT services.**

1.3 Audience

The intended audience of this document is:

- **IoT Service providers (e.g. Automakers, Utilities, Smart Cities etc.) who wish to understand how SIM based security technology can be used to enhance the security of their services.**
- **Mobile Network Operators who wish to offer enhanced SIM based IoT authentication services to IoT service providers.**
- **Technology vendors that supply Mobile Network Operators and IoT service providers with security technologies.**

2 Explaining the IoT Authentication Challenge

2.1 Growth of Non-Cellular IoT Devices

In the next 10 years, the number of IoT devices is expected to grow exponentially. One forecast published in August 2016 by Machina Research [20] predicts that by 2025, there will be a total of 27 billion IoT devices; of these, 2.2 billion devices are expected to be connected via cellular networks (e.g. GSM, UMTS, LTE), 2.9 billion devices will connect via low power wide area networks (e.g. EC-GSM-IoT, NB-IoT, LTE-MTC) and 19 billion devices will connect via short range "non-cellular" wireless technologies (e.g. Wi-Fi, Bluetooth, ZigBee, and Z-Wave).

The IoT devices that connect via non-cellular technologies will include sensors, actuators and other resource-restrained devices with limited memory, intelligence and user interfaces.
Most non-cellular devices will gain connectivity via a local area connection to a wide area network gateway device.
Multiple authentication mechanisms for such connectivity is available today, developed by various industry alliances and standardisation bodies such as Bluetooth SIG, ZigBee Alliance, LoRa Alliance, 3GPP, IEEE, etc.

These authentication mechanisms usually only cover the connection between the non-cellular device and the gateway, and this can impose a major security challenge within the service as further explained below.

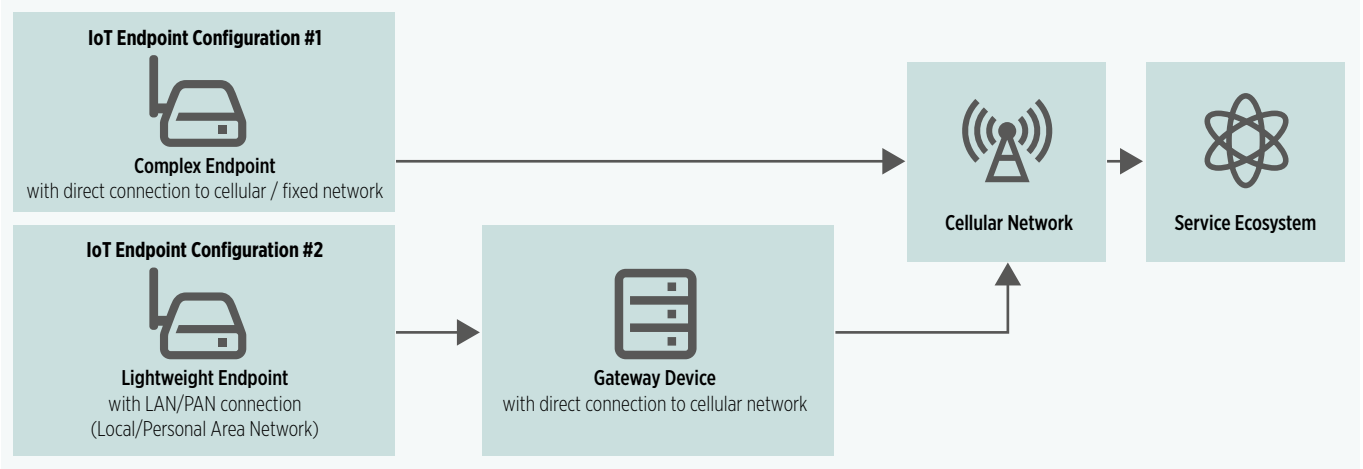
2.2 IoT Service Architectures and their Authentication Challenges

Deployments of IoT services, which combine the connection of cellular and non-cellular devices, are frequently required for IoT services. For example, short-range non-cellular devices are extensively used for healthcare and home automation services that require low power consumption, long battery life and lower cost compared to cellular devices. These non-cellular devices connect to a gateway or concentrator that uses cellular or fixed connectivity to a WAN (Wide Area Networks). Connected cars are another scenario, where a cellular enabled telematics unit in a car essentially acts as a communications gateway for other local devices connected to the car's CAN (Controller Area Network) bus.

IoT service providers typically adopt one of two different service architectures depending upon the cost target of their devices and the environments into which the devices are to be deployed. These typical IoT service configurations are shown in figure 1 below.

For each configuration we need to consider how secure authentication of the device is achieved at both the communication and application layers of the IoT service. As a first step it is worth considering how authentication is typically implemented within these two configurations today and what issues this might pose to the IoT service provider.

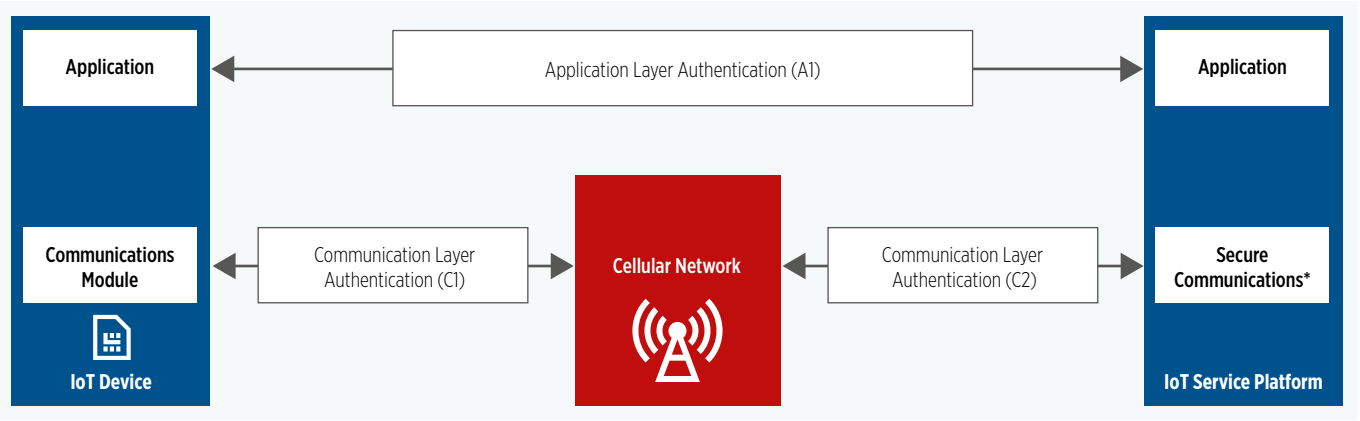
FIGURE 1: TYPICAL IoT CONFIGURATIONS



2.2.1 IoT Service Configuration #1

The communication and application authentication layers for IoT Service Configuration #1 are shown in the diagram below:

FIGURE 2: IoT SERVICE CONFIGURATION #1



For communication layer authentication:

- **C1 - The SIM card (for a cellular enabled device) is authenticated by the cellular network (e.g. using Milenage [4]).**
- **C2 - If the IoT service is using a private channel then there may also be authentication between the cellular network and the IoT service platform (e.g. using IPsec).**

For application layer authentication:

- **A1 - There is mutual authentication between the IoT application on the device and service platform application (e.g. using Transport Layer Security (D/TLS)).**

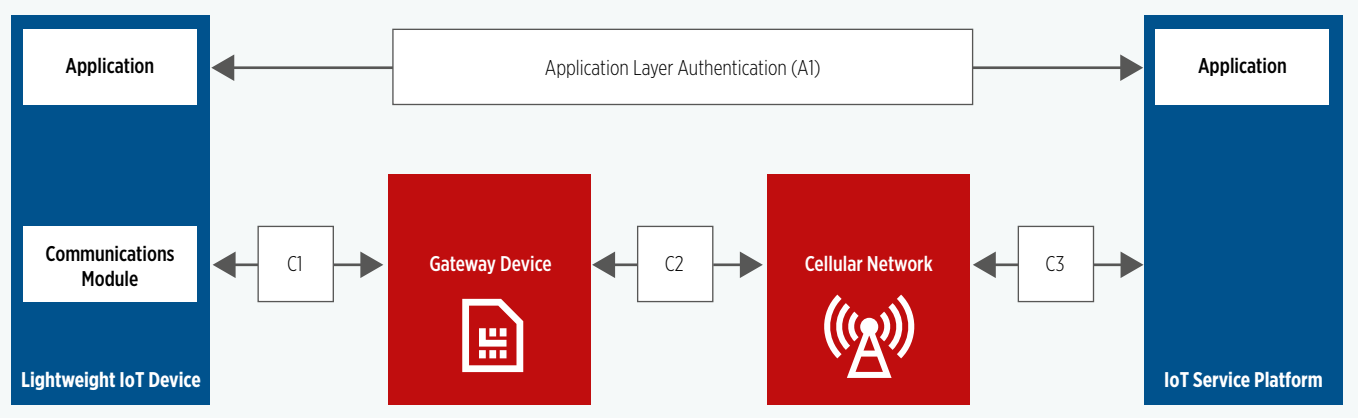
Authentication Challenge:

- **In this scenario the communication layer authentication between the device and the cellular network is managed by the Mobile Network Operator. The principle challenge for the IoT service provider is how to provision, protect and manage the application layer security (A1) .**

2.2.2 IoT Service Configuration #2

The communication and application authentication layers for IoT Service Configuration #2 are shown in the diagram below:

FIGURE 3: IoT SERVICE CONFIGURATION #2



For communication layer authentication:

- **C1 - The communications module is authenticated to the gateway (e.g. using 802.11 WPA2 Personal / WPA2 Enterprise, ZigBee AES etc.).**
- **C2 - The SIM card in the cellular enabled gateway is authenticated by the cellular network (e.g. using Milenage).**
- **C3 - If the IoT service is using a private channel then there may also be authentication between the network and the IoT service platform (e.g. using IPsec).**

For application layer authentication:

- **A1 - There is mutual authentication between the IoT application on the device and service platform application (e.g. using D/TLS).**

Authentication Challenges:

- **Discovery of Gateway (and the Gateway's services) by the IoT device.**
- **How to securely establish cryptographic keys between the IoT Device and the Gateway Device.**
- **How to avoid a "Man-in-the-Middle" attack between the Gateway and the lightweight IoT Device.**
- **How to ensure the integrity of the firmware within the Gateway.**
- **How to provision, protect and manage both the communication and application layer authentication credentials within the IoT device.**
- **How the credentials are protected at the lightweight device and which cryptographic algorithms and protocols are supported by the lightweight device.**

2.3 The Challenge of Protecting Certificates

Certificates, for authentication in the application layer using D/TLS in the two configurations described above, rely on a Public Key Infrastructure (PKI) for authentication and asymmetric cypher suites for tunnelling and encryption.

The security of a certificate based system relies on the secrecy of the private key that it is "provisioned" within the device. The technique used to provision the private key is crucial for future security. If the device is capable, it is preferable for the private-public key pair to be generated within a secure part of the device itself. If private keys have to be generated externally to the devices, then a secure process needs to be established to provision them in the devices.

If the private-public key pair is generated within a secure part device. The device will later on generate a CSR (Certificate Signing Request) that will be sent to a RA/CI that will generate its certificate. The certificate will be sent back to the device, as explained later in this section.

A public key must also be generated at the same time as the private key. This public key has to be registered and stored in a Registration Authority node for further authentication. During this registration process the device obtains a signed certificate from the Registration Authority. This signed certificate, although not mandatory, is desirable for maintaining the integrity of the information from the given device until the certificate is revoked.

In both cases, a SIM card supporting asymmetric cryptography provides an adequate solution to provision certificates and externally generated key pairs, and / or generate new key pairs on-board. A SIM card can fully secure their usage by performing associated cryptographic operations such as authentication, encryption/decryption and digital signature in a tamper resistant manner. Such capabilities can be supported in application-dependent security domains within a SIM Card, and can co-exist with the standard security features based on symmetric keys.

For a SIM-capable device, an applet on a SIM could generate a private/public key pair and provide the public key to the device. The device would then generate a Certificate Signing Request (CSR) with the public key, request the SIM to sign the CSR, and then send the signed-CSR to the Certificate Issuer (CI) to request a certificate. Upon receipt of a certificate, the device would inject this certificate into a security domain within the SIM.

The certificate could, for example, be used to establish end to end security between the IoT Service Provider and the Security Domain within the SIM Card using secure channel protocols like SCP11 [11]. It can also be used to establish a secure channel between the IoT device and the service provider.

2.4 Summarising the IoT Authentication Challenge

If every IoT service provider deploys a proprietary application layer authentication mechanism, the already existing market fragmentation will grow further, increasing costs of solution maintenance and device replacement, and potentially increasing security risks. As more small players start using IoT solutions, they will need support in implementing secure mechanisms for application layer authentication.

In the varied network deployment scenario mentioned above, the authentication of non-cellular devices will be an integral part of emerging end-to-end security requirements for IoT services. Therefore, if non-cellular devices are connected to cellular enabled gateways and not set up or authenticated correctly, they could create potential security threats leading to loss of customer data, connection of rogue devices and/or other issues.

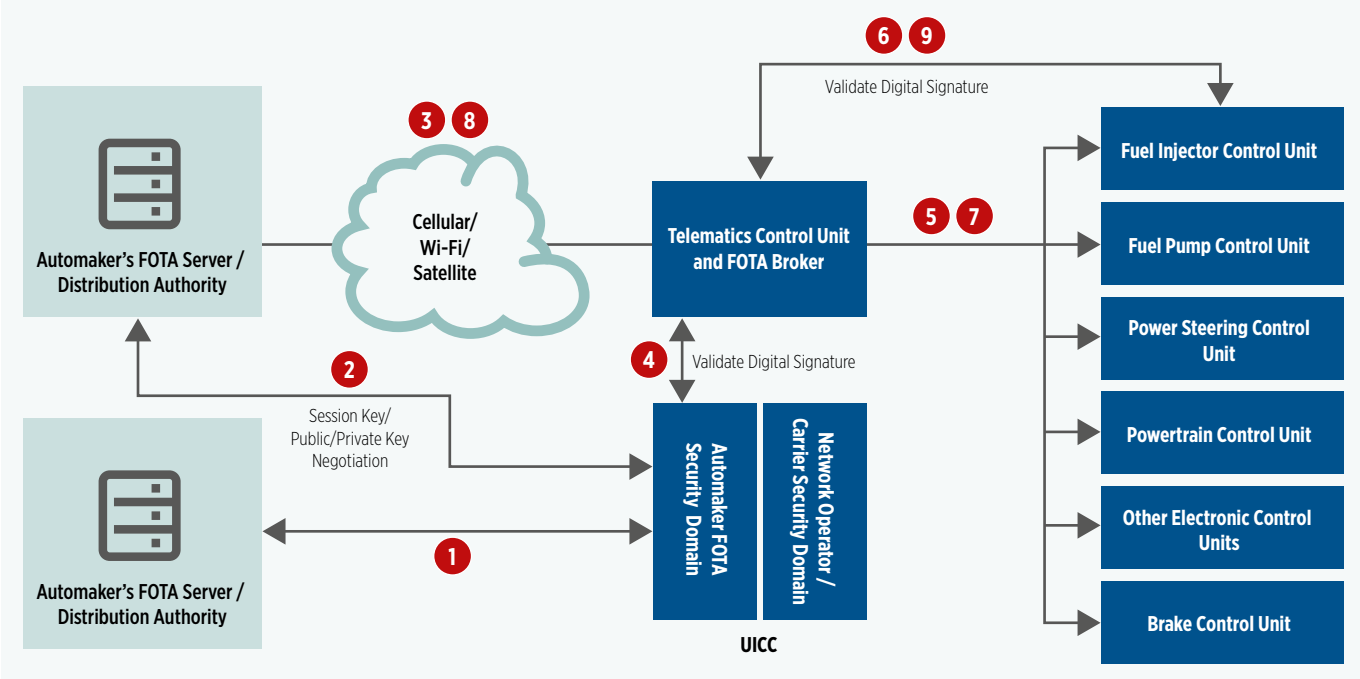
3 Example Use Cases

This section describes two use cases that are enhanced through the use of SIM cards.

3.1 Using a SIM Card to Verify the Integrity of Firmware Updates

The figure below demonstrates how, using the SIM card based security domains described in section 4.1, the security of an automotive over-the-air firmware update can be enhanced.

FIGURE 4: PROCESS FLOW FOR SIM CARD (UICC) TO VERIFY THE INTEGRITY OF AUTOMOTIVE OVER-THE-AIR FIRMWARE UPDATES



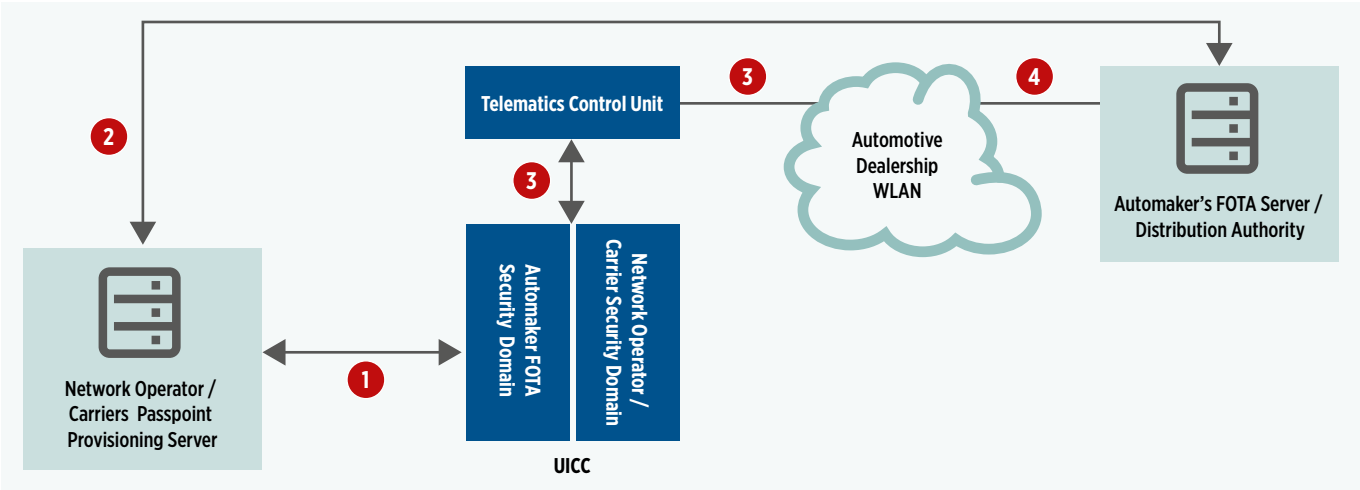
The process flow is as follows:

1. A dedicated security domain for the Automaker's FOTA service is created within the SIM card (the operator profile in the case of an eUICC) by the Network Operator that issued the SIM to the Automaker. The credentials to remotely and independently administer the security domain are passed securely to the Automaker's FOTA server.
2. A secure channel is established between the Automaker's FOTA server and the Automaker's security domain within the SIM card. FOTA credentials are loaded by the Automaker's FOTA server into the security domain.
3. A FOTA package is pushed from Automaker's FOTA distribution authority to the FOTA broker within a vehicle's TCU. The package is secured using the FOTA credentials.
4. The digital signature of the FOTA package is validated using the credentials within the Automaker's FOTA security domain.
5. If valid, the FOTA package is pushed from the FOTA Broker to the target ECU or module over the CAN bus within the vehicle.
6. Once received by the target ECU the digital signature of the FOTA package is validated by the ECU using the credentials within the FOTA security domain within the SIM card.
7. The target ECU reports the status of the firmware update to the FOTA broker:
   a) "Update applied OK" or
   b) "Update not applied – Error"
8. The FOTA broker relays the status of the firmware update to the Automaker's FOTA Distribution Authority.
9. On a periodic basis, the integrity of each ECU's firmware can be re-checked using the firmware credentials stored within the SIM card.

3.2 Using a SIM Card to Connect and Authenticate to a Trusted WLAN

In this automotive IoT scenario data traffic is offloaded to a trusted WLAN when the car arrives at a dealership to be serviced. The process for Wi-Fi offload using a SIM card in conjunction with Passpoint and EAP-AKA [28] is shown below:

FIGURE 5: PROCESS FLOW FOR WI-FI OFFLOAD USING A SIM CARD IN CONJUNCTION WITH PASSPOINT AND EAP-AKA [28]



1. In addition to providing the SIM card, the network operator provisions Passpoint data onto the SIM card as part of the Wi-Fi configuration in the vehicle. The Passpoint data includes information that allows the Wi-Fi radio to discover and connect to a trusted Wi-Fi network automatically. The SIM is also provisioned with Wi-Fi access credentials to enable EAP-AKA [28] authentication of the Wi-Fi network.
2. The network operator provides (or works with roaming partners to provide) trusted Wi-Fi network access at car dealerships.
3. When the vehicle pulls into a car dealership, the automobile uses the Passpoint subscription information stored in its SIM card to select and connect to the Wi-Fi network securely.
4. The vehicle authenticates the Wi-Fi network using EAP-AKA [28] credentials stored in its SIM card.
5. The vehicle establishes application connectivity to the automobile manufacturer's diagnostics server.

4 Solutions to Solve the IoT Authentication Challenge

4.1 Solving the Authentication Challenge Using Security Domains

4.1.1 Use of Application Specific Security Domains in Cellular Enabled IoT Devices

In the case where a cellular enabled device is used in the above scenarios, independently of the application specific security requirements, IoT devices or gateways that directly connect to a cellular network will implement an interface towards a SIM card as specified in ETSI TS 102 221 [10].

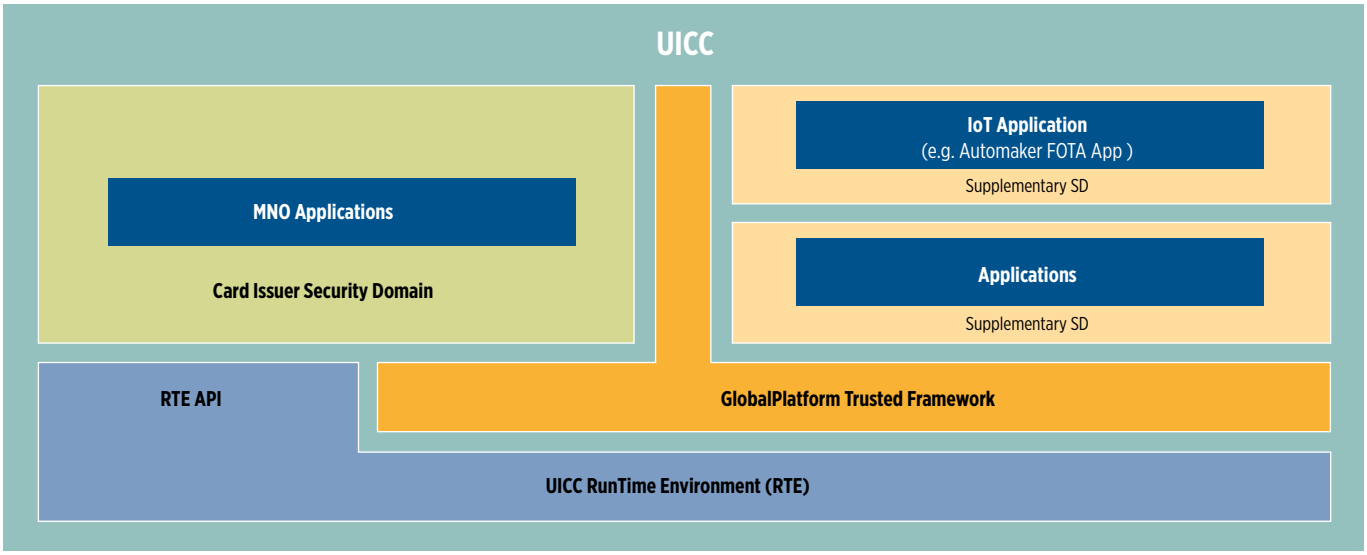
A SIM card provides tamper resistant protection to secrets used to protect access to sensitive assets during computing and storage. Thereby, they have been successful at preventing cloning of credentials, a capability desirable to cellular network operators, but also required in IoT applications where devices are physically accessible to attackers, either because their users find a financial incentive to break the security (e.g. Smart Meters), or because they are not under constant physical protection by their owners, providing opportunities to malevolent parties (house burglary, auto theft etc.).

Beyond being used by MNOs to secure access to their network, the SIM card is intended as a multi-application secure computing platform that can support the provisioning and remote administrative requirements of multiple independent stakeholders.

Therefore, stakeholders (such as wireless network operators) deploying SIM cards can leverage their investment by lending SIM capabilities to meet the security needs of their IoT service provider customers. Such a model is beneficial as it spares the IoT service provider from having to design and provision an alternative means to address the security needs of their IoT devices by reusing the hardware capabilities of the SIM card. Furthermore SIM cards provide a standardised framework to securely provision and manage sensitive data and applications on remote devices through their lifecycle, enabling IoT service providers to leverage the existing remote administration infrastructure that may be deployed by their MNO partner.

One important feature of a GlobalPlatform enabled SIM card is its ability to support multiple isolated and independent security domains. Through this feature, IoT service providers can independently store and administer their own security credentials within the SIM, which can then be used by other components within the IoT system. For example, a SIM card intended to serve a cellular IoT device could include the following:

FIGURE 6: EXAMPLE CONFIGURATION OF SECURITY DOMAINS INSIDE A UICC



- **One Security Domain under the responsibility of the Mobile Network Operator, typically provisioned with e.g. a USIM application as specified in 3GPP TS 31.101 [1] and TS 31.102 [2] to manage network access.**
- **Another Security Domain under the responsibility of an IoT Service Provider, possibly provisioned with e.g. a oneM2M Service Module (1M2MSM) application as specified in Annex D of oneM2M TS-0003 [23], or an M2MSM application as specified in ETSI SmartM2M TS 102 921 [6], to manage access to an M2M service layer.**
- **Possibly several other security domains managed by e.g. the IoT device manufacturer to provision personalized device configuration information, or by IoT application vendors to provision application specific credentials and profiles as described in section 2.3.**

The security domains would be organised hierarchically under the responsibility of the stakeholder issuing the SIM (or operator profile in the case of an eUICC), which may vary depending on vertical ecosystems and market agreement. The most common scenario is that a network operator would rent a supplementary security domain within the SIM to an IoT service provider who would provision its own application and, possibly, allocate any remaining space to their application providers. In other scenarios, the SIM platform may come pre-embedded in the device by an equipment vendor (e.g. an automaker), and the SIM resources would be allocated to the network operator and IoT service providers chosen by the customer upon deployment, as enabled by the GSMA Embedded SIM specifications [18] [19].

Not only can security domains be initially provisioned as instructed by their respective owners, but they can also be remotely administered over their lifetime provided that an Over-the-Air (OTA) Remote Administration infrastructure (as specified by ETSI TS 102 225 [9]/ TS 102 226 [8]) has been deployed to manage the SIM card. The remote administration of SIM cards is possible Over the Air (OTA) e.g. through use of SMS and IP connections using HTTP. This framework enables establishment of end-to-end secure channels between the stakeholder owning a security domain and their managed security domains on SIM cards within the IoT devices. Through this secure channel, the stakeholder has the following capabilities:

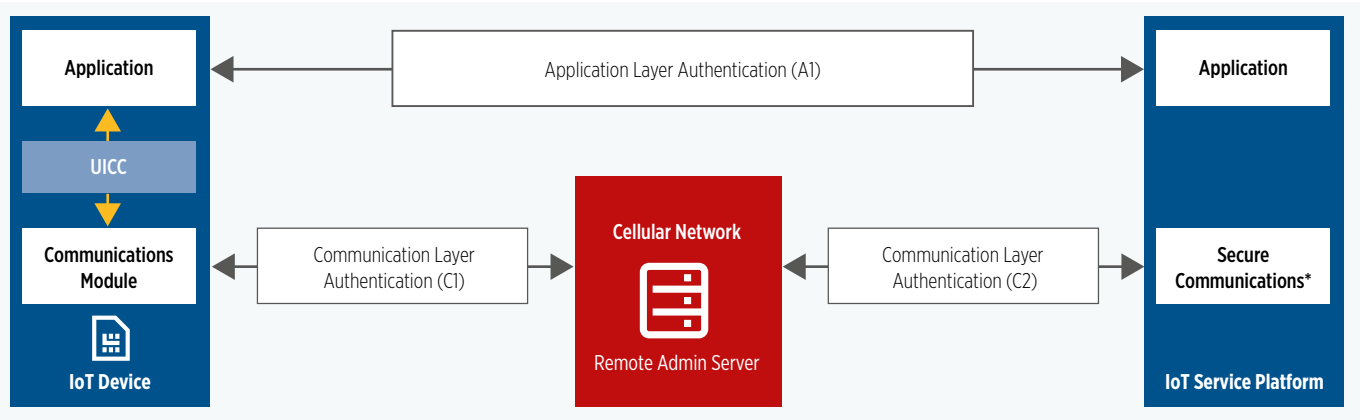
- **Administration of Javacard applications in the security domain (loading, installation and deletion of stakeholder specific applets that interact with the device through the SIM toolkit specified in ETSI TS 102 223 [7]).**
- **Administration of information provisioned in the SIM file system through remote file management command scripts as specified by ETSI and GlobalPlatform. Provided the mapping of managed information on a SIM card file system structure has been specified, the management scripts should be interoperable across SIM cards from different manufacturers.**

The administration commands are interoperable between SIM cards of different manufacturers provided the SIMs comply with GlobalPlatform Card Specification v2.2.1 [12] or higher. This specification includes specific configuration information for SIMs to enable creation and personalization of Security Domains as well as setting up dedicated secure channels through the infrastructure to their administrating stakeholder. The back-end infrastructure to remotely administer SIM cards, supporting the secured packet protocol of ETSI TS 102 225 [9], is generally deployed by Mobile Network Operators. The GlobalPlatform Confidential Card Content Management [13] specification provides a way for a third party stakeholder to administer their own security domain independently through the use of this common infrastructure, thanks to the confidential setup of secure channel keys. Both push and pull mechanisms are supported to trigger the administrative sessions between the stakeholder's platform and the connected devices.

This assumes SIM cards supporting GlobalPlatform Card Specification [12] 2.2.1 or higher with Confidential Card Content Management and remote administration capabilities as specified in ETSI TS 102 226 [8]. The issuer of such SIM cards (typically the Network Operator) has the capability to delegate rights to manage specific security domains with pre-configured resources to other stakeholders.

The above framework addresses the challenges encountered by IoT Service providers or device/application providers for credential management and secure connection establishment in the IoT Service Configuration #1 exposed in section 2.2.1.

FIGURE 7: IoT SERVICE CONFIGURATION #1 WITH SIM CARD BASED SECURITY DOMAIN ENHANCEMENT



Through this technology IoT service providers can leverage the Mobile Network Operator infrastructure and personalisation chain to provision custom (non-network operator) application specific credentials onto the SIM card, which then enables:

- **Use of the SIM card as a trust anchor to verify the integrity of other components within the IoT service architecture.**
- **Use a SIM card to facilitate the deployment and management of public/private key pairs (as needed e.g. for application layer security) to other components within the IoT service architecture.**

Within the oneM2M standards, a framework supporting the initial provisioning and remote administration of IoT specific credentials and configuration information, as well as GBA based application key derivation and authentication, is specified in Annex D of oneM2M Security Solutions TS-0003 [23]. Though this framework leaves flexibility to be tailored according to the need of specific deployments, it is sufficient to enable interoperability for the provisioning and remote administration of oneM2M contextual information across all supporting devices.

For this approach to become attractive to IoT application developers, it will be necessary to provide them with a simple API to facilitate actual usage of the SIM deployed credentials and associated capabilities in the device application code. To really enable the deployment of secure IoT solutions relying on tamper resistant components such as the SIM, the use of such components should become transparent to application developers. For this purpose, oneM2M is conducting a work item "Secure Environment Abstraction Layer" which will enable IoT devices to access the functionalities of secure environments through a uniform API regardless of their implementation - be it a discrete component such as a SIM card, other embedded security module or Trusted Platform Module, Trusted Execution Environment, or software depending on desired security level.

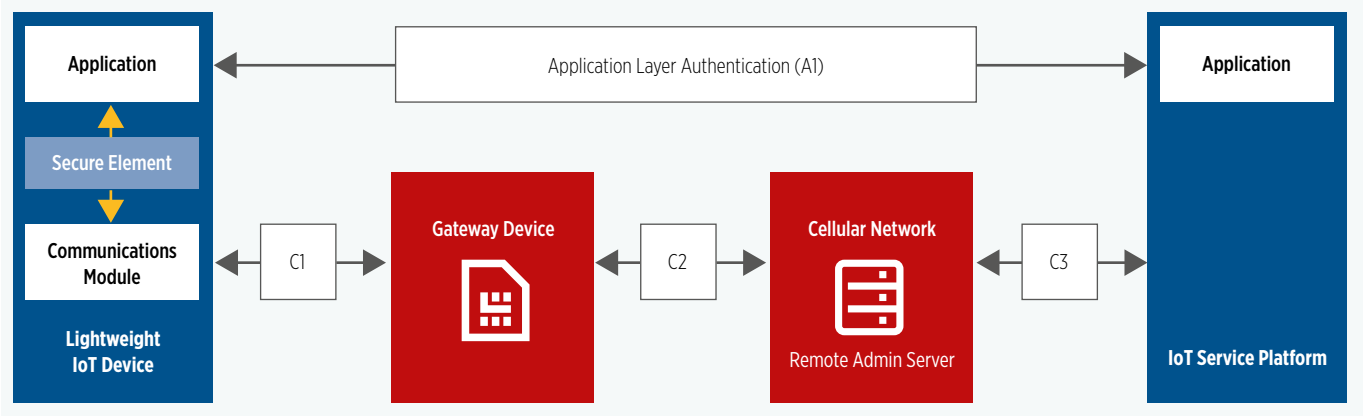
IoT devices can also utilize SIMalliance OMAPI [24] and GlobalPlatform Secure Element Access Control [14] to ensure that only authorized applications are able to perform I/O operations with the secure element. Access is governed by policy rules stored in the Access Rule Application (ARA) of the secure element. The device operating system has the responsibility to enforce the rules defined within the SIM card.

4.1.2 Extension for GlobalPlatform Enabled Non-Cellular IoT Devices

In IoT service configuration #2 (as described in section 2.2.2), the IoT device has no direct communication to a cellular network, and may need to go through one or more intermediate hops to reach a WAN infrastructure.

Though not typically equipped with SIM cards, non-cellular devices supporting security sensitive applications should still embed a security Root of Trust. This may take the form of a Secure Element (when physical protection is desired) or an integrated Trusted Execution Environment (when mostly remote protection is expected) compatible with GlobalPlatform Specifications. As long as the communication link between the Gateway and the non-cellular device supports HTTP, the existing GlobalPlatform back-end infrastructure (e.g. deployed by a Mobile Network Operator for SIM management) can be naturally extended to address such secure components (Secure Element or Trusted Execution Environment), provided the stakeholder managing the back-end infrastructure offers the possibility to provision such components through this infrastructure.

FIGURE 8: IoT SERVICE CONFIGURATION #2 WITH SECURE ELEMENT BASED SECURITY DOMAIN ENHANCEMENT



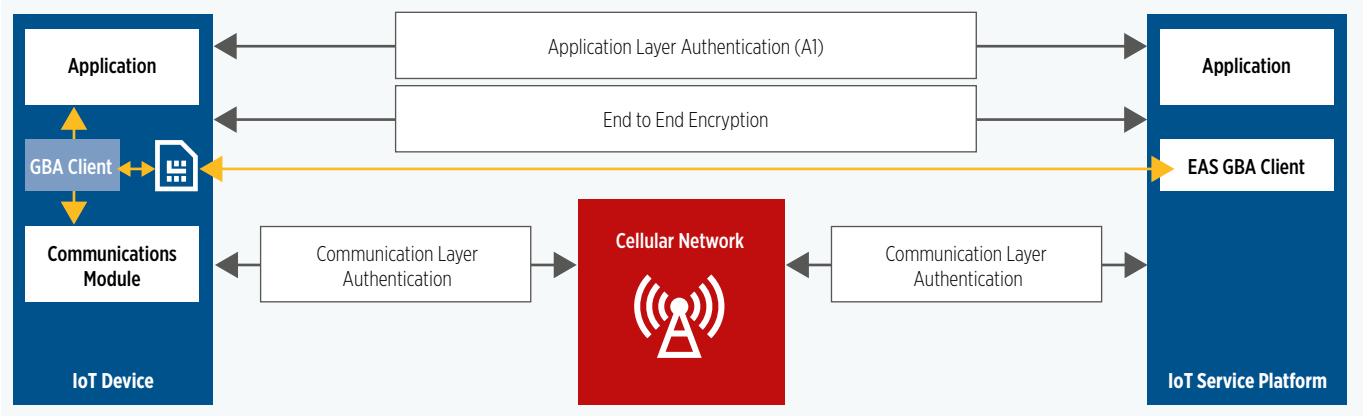
It is worth noting that this configuration can be generalized to any communication means between the lightweight IoT device and the IoT Service Platform, such as wireline IP or other means that do not use a cellular enabled gateway device. The network operator's ability to provision and remotely administrate credentials on secure elements could be extended to cover non-cellular scenarios.

In case of a Secure Element (SE), the SE hosting device needs to support an appropriate interface and API as defined in the GlobalPlatform specification to enable remote administration.

4.2 Solving the Authentication Challenge Using GBA

Another feature that a SIM card capable device has is the possibility to implement a Generic Bootstrapping Architecture (GBA) [3] client. GBA allows mutual authentication of a device with EAS (Enterprise Application Software). The advantages of GBA is that the device can automatically authenticate using SIM card stored credentials and thus create a unique, time limited, session key that can further be used for setting up a secure TLS tunnel with the EAS. The TLS connection is end to end, and does not require pre-provisioning of certificates since the TLS is based on a PSK symmetric cypher suite where the shared secret is the time limited GBA session. IoT device configuration #1 can be expanded with GBA to look as follows:

FIGURE 9: IoT SERVICE CONFIGURATION #1 WITH GBA ENHANCEMENT



Another advantage of GBA is that GBA is IP based hence any protocol based on IP can therefore implement GBA. In this case, all communication network technologies (e.g. Cellular, Wi-Fi, Bluetooth etc.) that already have IP can support GBA authentication and encryption.

4.3 Using a SIM Card to Offload IoT Traffic to a WLAN Using Passpoint™

Some Mobile Network Operators can offload traffic to Wi-Fi networks to extend coverage and take advantage of localised Wi-Fi network bandwidth for data transfer. Offloading reduces the amount of data being carried on the cellular networks, freeing bandwidth for other cellular users.

Wi-Fi network offload, particularly for headless IoT devices, is challenging in that user interaction may be required to discover and connect to a Wi-Fi network. Furthermore, not all Wi-Fi Hotspots are secure, so connecting to an insecure Wi-Fi hotspot may compromise the security of an IoT device.

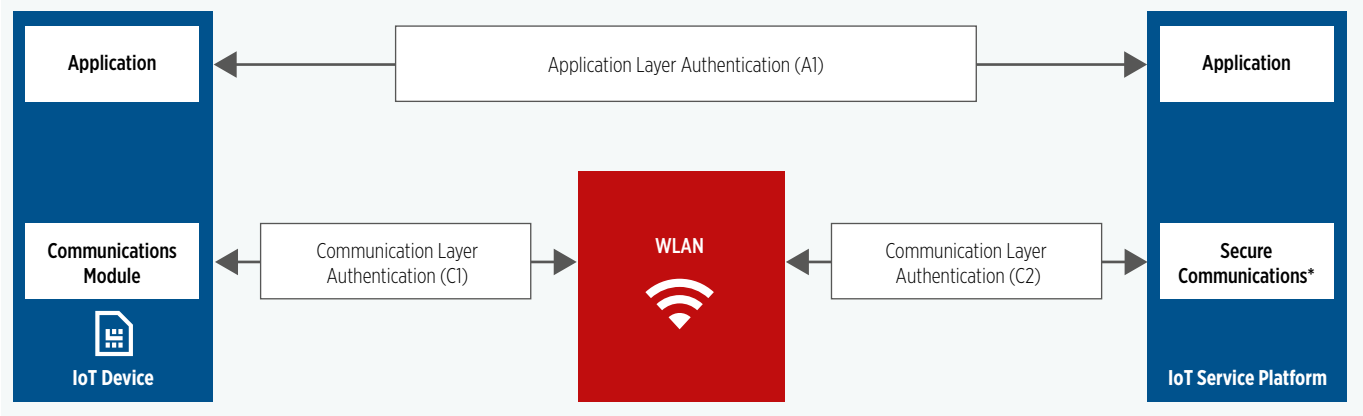
Passpoint™ [25] technology provides a means for mobile network operators to provision Wi-Fi network policy information into an IoT device, allowing it to discover Wi-Fi networks and establish secure connectivity to a Wi-Fi network using EAP-SIM, EAP-AKA [28] or EAP-AKA' authentication.

The figure below demonstrates how the SIM card based authentication could be used to offload traffic to a secure WLAN.

To provide an example for the use of this capability, in an automotive IoT scenario, traffic could be offloaded: when the user is refuelling an automobile; or when they arrive at a car dealership to have their automobile serviced.
Passpoint provides the capability for an IoT device to:

- **Use seamless WPA2-Enterprise [30] ™ authentication.**
- **Enable the user device to "see behind the Service Set Identity (SSID)" and connect to the network operator, not the hotspot.**
- **Passpoint allows the network operators to:**
- **Provision a single subscription that will allow an IoT gateway to establish network access at Wi-Fi hotspots**
- **Provision subscriber-specific policies**
- **Provide agreements with other network operators for Wi-Fi access at their hotspots through use of the provisioned subscription.**

FIGURE 10: USING A SIM CARD TO OFFLOAD TO A WLAN



5 Definitions, Abbreviations and References

5.1 Definitions

Term	Description
GlobalPlatform	GlobalPlatform is an association which defines and develops specifications to facilitate the secure deployment and management of multiple applications on secure chip technology.
Internet of Things	The Internet of Things (IoT) describes the coordination of multiple machines, devices and appliances connected to the Internet through multiple networks. These devices include everyday objects such as tablets and consumer electronics, and other machines such as vehicles, monitors and sensors equipped with communication capabilities that allow them to send and receive data.
Root of Trust	A set of cryptographic policies and procedures that govern how identities, applications, and communications can and should be cryptographically secured.
Secure Element	Tamper-resistant dedicated platform, consisting of hardware and software, capable of securely hosting applications and their confidential and cryptographic data and providing a secure application execution environment, e.g. a UICC.
SIM Card	A UICC (see below) that may or may not be Remotely Provisionable as per the GSMA Remote Provisioning Specification [18] [19].
UICC	A Secure Element platform specified in ETSI TS 102 221[10] that can support multiple standardized network or service authentication applications in cryptographically separated security domains. It may be embodied in embedded form factors specified in ETSI TS 102 671 [5].

5.2 Abbreviations

Term	Description
3GPP	3rd Generation Project Partnership - www.3gpp.org
API	Application Programming Interface
ARA	Access Rule Application
CAN	Controller Area Network
CLP	GSMA Connected Living Programme – www.gsma.com/iot
CPE	Customer Premises Equipment
DPP	Device Provisioning Protocol
EAP-SIM	Extensible Authentication Protocol Subscriber Identity Module
EAP-AKA	Extensible Authentication Protocol Authentication and Key Agreement
EAP-AKA'	Extensible Authentication Protocol Authentication and Key Agreement Prime
EAS	Enterprise Application Software
ETSI	European Telecommunications Standards Institute
eUICC	Embedded UICC
FOTA	Firmware Over The Air
GBA	Generic Bootstrapping Architecture
GSMA	GSM Association – www.gsma.com
HSM	Hardware Security Module
IEEE	Institute of Electrical and Electronic Engineers – www.ieee.org
IoT	Internet of Things
IPsec	Internet Protocol Security
LAN	Local Area Network
MNO	Mobile Network Operator

OMA	Open Mobile Alliance
OMAPI	Open Mobile Application Programming Interface
OTA	Over The Air
PAN	Personal Area Network
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
SD	Security Domain
SE	Secure Element
TEE	Trusted Execution Environment
TLS	Transport Layer Security
WAN	Wide Area Network
WLAN	Wireless Local Area Network

5.3 References

Ref	Doc Number	Description
[1]	**TS 31.101**	ETSI Machine-to-Machine communications; mla, dla and mld interfaces – www.etsi.org/
[2]	**TS 31.102**	ETSI Smart Cards; Card Application Toolkit – www.etsi.org/technologies-clusters/technologies/smart-cards
[3]	**TS 33.220**	ETSI Smart Cards; Remote APDU structure for UICC based applications – www.etsi.org/technologies-clusters/technologies/smart-cards
[4]	**TS 35.201**	ETSI Smart Cards; Secured packet structure for UICC based applications www.etsi.org/technologies-clusters/technologies/smart-cards
[5]	**TS 102 671**	ETSI Smart Cards; Machine to Machine UICC; Physical and logical characteristics www.etsi.org/technologies-clusters/technologies/smart-cards
[6]	**TS 102 921**	ETSI Machine-to-Machine communications; mla, dla and mld interfaces – www.etsi.org/
[7]	**TS 102 223**	ETSI Smart Cards; Card Application Toolkit – www.etsi.org/technologies-clusters/technologies/smart-cards
[8]	**TS 102 226**	ETSI Smart Cards; Remote APDU structure for UICC based applications – www.etsi.org/technologies-clusters/technologies/smart-cards
[9]	**TS 102 225**	ETSI Smart Cards; Secured packet structure for UICC based applications www.etsi.org/technologies-clusters/technologies/smart-cards
[10]	**TS 102 221**	ETSI Smart Cards; UICC-Terminal interface; Physical and logical characteristics www.etsi.org/technologies-clusters/technologies/smart-cards
[11]	**na**	GlobalPlatform Card Secure Channel Protocol '11' Card Specification v2.2 – Amendment F www.globalplatform.org/specificationscard.asp
[12]	**na**	GlobalPlatform Card Specification – www.globalplatform.org/specificationscard.asp
[13]	**na**	GlobalPlatform Confidential Card Content Management Specification – www.globalplatform.org/specificationscard.asp
[14]	**na**	GlobalPlatform Secure Element Access Control – https://www.globalplatform.org/specificationsdevice.asp
[15]	**CLP.13**	GSMA IoT Security Guidelines for Endpoint Ecosystems www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

[16]	**CLP.12**	GSMA IoT Security Guidelines for Service Ecosystems – www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[17]	**CLP.11**	GSMA IoT Security Guidelines Overview Document – www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[18]	**SGP.02**	GSMA Remote Provisioning Architecture for Embedded UICC – www.gsma.com/iot/embedded-sim/
[19]	**SGP.22**	GSMA RSP Technical Specification – www.gsma.com/newsroom/all-documents/sgp-22-v2-0-technical-specification/
[20]	**na**	Machina IoT Global Forecast & Analysis 2015-2025 report machinaresearch.com/news/press-release-global-internet-of-things-market-to-grow-to-27-billion-devices-generating-usd3-trillion-revenue-in-2025/
[21]	**na**	OMA Device Management – technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases
[22]	**na**	OMA LightweightM2M - technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases
[23]	**TS-0003**	oneM2M Security Solutions – onem2m.org/technical/published-documents
[24]	**na**	SIMalliance Open Mobile API Specification – simalliance.org/key-technical-releases/
[25]	**na**	Wi-Fi Alliance® - "Passpoint - Operator Best Practices for AAA Interface Deployment – www.wi-fi.org/discover-wi-fi/specifications
[26]	**na**	Wi-Fi Alliance® - Wi-Fi Device Provisioning Protocol Technical Specification – www.wi-fi.org/discover-wi-fi/specifications
[27]	**RFC 4186**	IETF - Extensible Authentication Protocol Method for Global System for Mobile Communications Subscriber Identity Modules tools.ietf.org/html/rfc4186
[28]	**RFC 4187**	IETF - Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement tools.ietf.org/html/rfc4187
[29]	**RFC 5448**	IETF - Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement tools.ietf.org/html/rfc5448
[30]	**na**	Wi-Fi Alliance® - The State of Wi-Fi® Security www.wi-fi.org/download.php?file=/sites/default/files/private/20120229_State_of_Wi-Fi_Security_09May2012_updated_cert.pdf

6 Document Management

6.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	30 Nov 2016	1st Version	GSMA Internet of Things PET	Ian Smith / GSMA

6.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	30 Nov 2016	1st Version	GSMA Internet of Things PET	Ian Smith / GSMA

Floor 2, The Walbrook Building
25 Walbrook, London EC4N 8AF UK
Tel: +44 (0)207 356 0600

iot@gsma.com
www.gsma.com