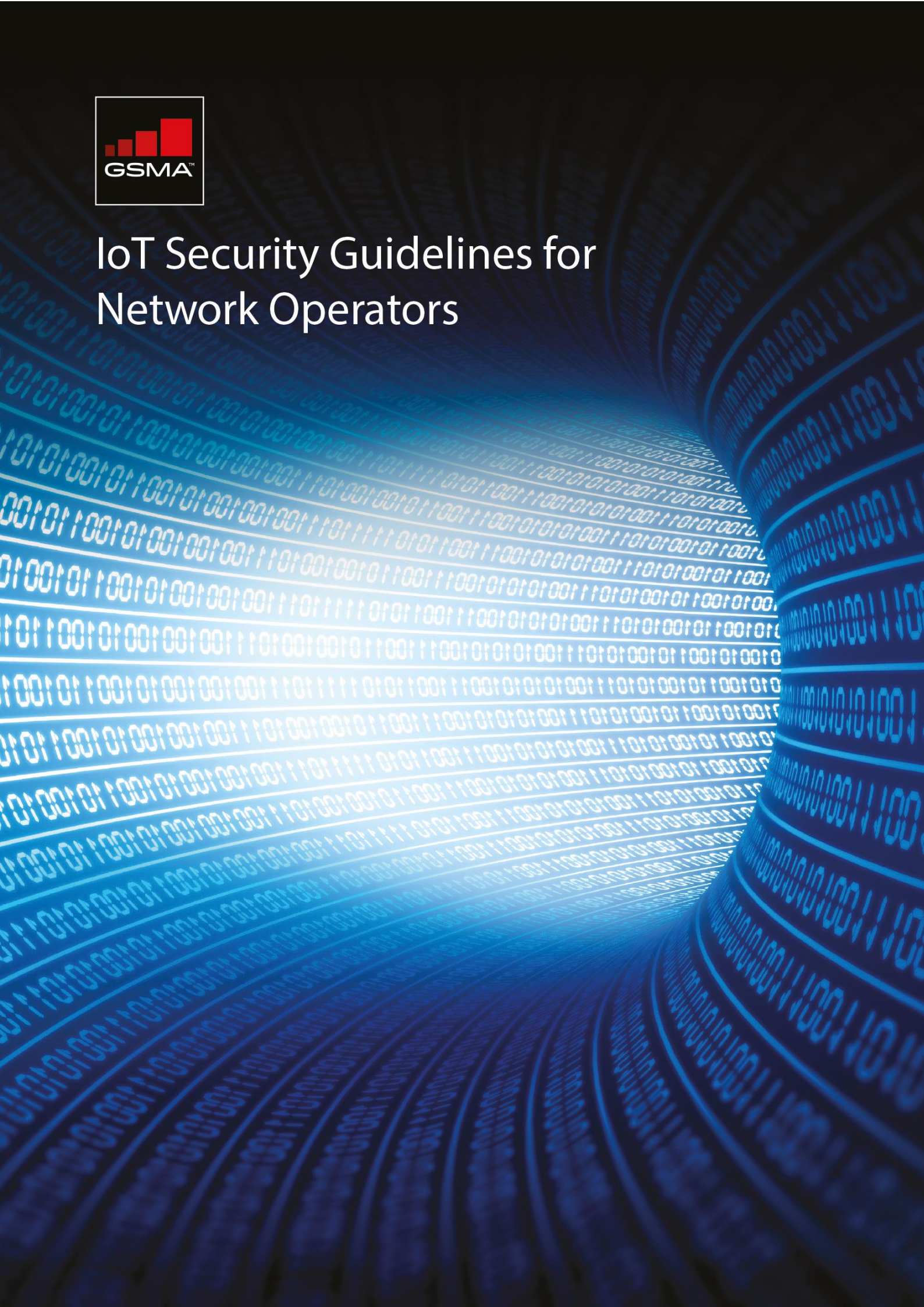
GSMA
IoT Security Guidelines for
Network Operators

IoT Security Guidelines for Network Operators

Version 1.1

07 November 2016

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2017 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

This document provides top-level security guidelines for Network Operators who intend to provide services to IoT Service Providers to ensure system security and data privacy. Recommendations are based on readily available systems and technologies that are deployed today.

1.2 Document Structure

This document is a document intended for Network Operators and IoT Service Providers. Readers of this document may also be interested in reading the other documents in the GSMA's IoT Security Guidelines document set [11], as shown below.

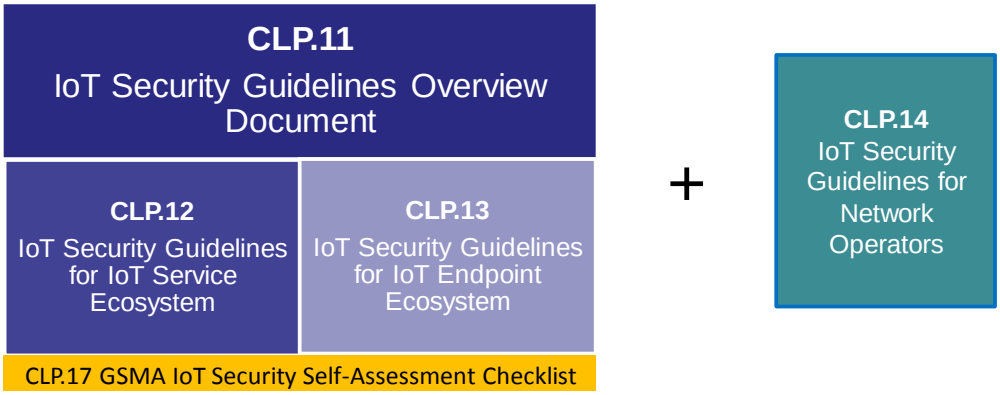

Figure 1- Structure of the GSMA IoT Security Guidelines Document Set

1.3 Document Purpose and Scope

This document should act as a checklist in the supplier agreements between IoT Service Providers and their Network Operator partner(s).

The scope of the document is limited to:

- Security guidelines related to IoT Services.
- Recommendations pertaining to the security services offered by a Network Operator.
- Cellular network technologies.

This document is not intended to create new IoT specifications or standards, but will refer to currently available solutions, standards and best practice.

This document is not intended to accelerate the obsolescence of existing IoT Services. Backwards compatibility with the Network Operator's existing IoT Services should be maintained when they are considered to be adequately secured.

This document does not address the security issues associated with the interfaces and APIs implemented on the IoT Service Platform (or IoT Connectivity Management Platform) in order for the IoT Service Platform to share its data with end users (for example to share data

with an end user via a smartphone or PC application) or other entities within the ecosystem. Such interfaces and APIs shall be secured using 'best practice' internet security technologies and protocols.

It is noted that adherence to national laws and regulations for a particular territory may, where necessary, overrule the guidelines stated in this document.

1.4 Intended Audience

The primary intended audience of this document is:

- Firstly, Network Operators who wish to provide services to IoT Service Providers.
- Secondly, enterprises and organisations who are looking to develop new and innovative connected products and services (the so called "Internet of Things") utilising cellular of fixed line networks. In this document we refer to these enterprises as "IoT Service Providers".

1.5 Definitions

Term	Description
Device Host Identify Reporting	A capability for an Endpoint device to report host information to a Network Operator. See GSMA Connection Efficiency Guidelines [17]
Diameter	Diameter is an authentication, authorization, and accounting protocol for computer networks. See IETF RFC 6733 [18]
Endpoint	An IoT Endpoint is a physical computing device that performs a function or task as part of an Internet connected product or service. See section 3 of CLP.13 [29] for a description of the three common classes of IoT devices, and examples of each class of Endpoint.
Gateway	A complex endpoint device that typically bridges between Lightweight Endpoint devices (connected via a local network) and a wide area network. See CLP.13 [29] for further information.
Internet of Things	The Internet of Things 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.
IoT Connectivity Management Platform	A system, usually hosted by the Network Operator, to allow the self-management of IoT subscriptions and price plans by the IoT Service Provider.
IoT Service	Any computer program that leverages data from IoT devices to perform the service.
IoT Service Platform	The service platform, hosted by the IoT Service Provider which communicates to an Endpoint to provide an IoT Service.
IoT Service Provider	Enterprises or organisations who are looking to develop new and innovative connected IoT products and services. The provider could be a Network Operator.
Lightweight Endpoint	Typically a constrained device (e.g. sensor or actuator) that connects to an IoT Service via a Gateway device.

Term	Description
Network Operator	The operator of the communication network that is connecting the IoT Endpoint device to the IoT Service Platform.
UICC	A Secure Element Platform specified in ETSI TS 102 221 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.
Wide Area Network	A telecommunications network that extends over a large geographical distance.

1.6 Abbreviations

Term	Description
3GPP	3rd Generation Project Partnership
AKA	Authentication and Key Agreement
APDU	Application Protocol Data Unit
API	Application Programming Interface
APN	Access Point Name
BGP	Border Gateway Protocol
CEIR	Central Equipment Identity Register
CERT	Computer Emergency Response Team
DNS	Domain Name System
DoS	Denial of Service
DPA	Data Processing Agreement
EAB	Extended Access Barring
EAP	Extensible Authentication Protocol
EID	eUICC Identity
ETSI	European Telecommunications Standards Institute
EU	European Union
eUICC	Embedded UICC
FASG	Fraud and Security Group
GCF	Global Certification Forum
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
GSM	Global System for Mobile communication
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
HSS	Home Subscriber Server
ICCID	Integrated Circuit Card Identity

Term	Description
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
L2TP	Layer Two Tunnelling Protocol
LBO	Local Break Out
LPWAN	Low Power Wide Area Network
LTE	Long-Term Evolution
M2M	Machine to Machine
MAP	Mobile Application Part
MME	Mobility Management Entity
OMA	Open Mobile Alliance
OSS	Operations Support System
OTA	Over The Air
PTCRB	A pseudo-acronym, originally meaning PCS Type Certification Review Board, but no longer applicable.
RAN	Radio Access Network
SAS	Security Accreditation Scheme
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMS	Short Message Service
SoR	Steering of Roaming
SS7	Signalling System No. 7
UMTS	Universal Mobile Telecommunications Service
USSD	Unstructured Supplementary Service Data
VLR	Visitor Location Register
VPN	Virtual Private Network
VoLTE	Voice over LTE
WAN	Wide Area Network

1.7 References

Ref	Doc Number	Title
[1]	ETSI TS 102 225	Secured packet structure for UICC based applications www.etsi.org
[2]	ETSI TS 102 226	Remote APDU structure for UICC based applications www.etsi.org

Ref	Doc Number	Title
[3]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application www.3gpp.org
[4]	N/A	Open Mobile API specification www.simalliance.org
[5]	OMA DM	OMA Device Management www.openmobilealliance.org
[6]	OMA FUMO	OMA Firmware Update Management Object www.openmobilealliance.org
[7]	GSMA SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification www.gsma.com
[8]	ETSI TS 102 310	Extensible Authentication Protocol support in the UICC www.etsi.org
[9]	3GPP TS 23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode www.3gpp.org
[10]	NISTIR 7298	Glossary of Key Information Security Terms www.nist.gov
[11]	GSMA CLP.11	IoT Security Guidelines Overview Document www.gsma.com
[12]	n/a	Introducing Mobile Connect – the new standard in digital authentication www.gsma.com/personaldata/mobile-connect
[13]	3GPP TS 34.xxx	3GPP 34 series specifications www.3gpp.org/DynaReport/34-series.htm
[14]	3GPP TS 37.xxx	3GPP 37 series specifications www.3gpp.org/DynaReport/37-series.htm
[15]	3GPP TS 31.xxx	3GPP 31 series specifications www.3gpp.org/DynaReport/31-series.htm
[16]	GSMA FS.04	Security Accreditation Scheme for UICC Production http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
[17]	GSMA CLP.03	IoT Device Connection Efficiency Guidelines www.gsma.com/iot/iot-connection-efficiency-guidelines-v4/
[18]	IETF RFC 6733	Diameter Base Protocol www.ietf.org
[19]	ETSI TS 102 690	Machine-to-Machine communications (M2M); Functional architecture www.etsi.org
[20]	TR-069	CPE WAN Management Protocol www.broadband-forum.org

Ref	Doc Number	Title
[21]	n/a	OpenID Connect openid.net/connect/
[22]	n/a	FIDO (Fast IDentity Online) Alliance fidoalliance.org/
[23]	ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface www.etsi.ord
[24]	n/a	National Institute of Standards and Technology (NIST) www.nist.gov
[25]	n/a	European Network of Excellence in Cryptology (ECRYPT) www.ecrypt.eu.org
[26]	GSMA CLP.12	IoT Security Guidelines for IoT Service Ecosystem www.gsma.com
[27]	IETF RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) tools.ietf.org/html/rfc5448
[28]	IETF RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) tools.ietf.org/html/rfc4186
[29]	GSMA CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem www.gsma.com
[30]	n/a	Wireless Security in LTE Networks www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf
[31]	GSMA CLP.17	IoT Security Assessment Checklist www.gsma.com/iot/iot-security-assessment/

2 IoT Service Assets That Network Operators Can Protect

The security features that need to be implemented to adequately protect IoT Service assets are specific to each service. Therefore, it remains the responsibility of the IoT Service Provider to use proper risk and privacy impact assessment processes to derive their specific security needs. Network Operators and IoT Service Providers often share similar security requirements to protect their assets, therefore it makes sense for them to leverage on common security solutions rather than implementing duplicate (and potentially redundant) security infrastructures. Moreover, in many cases the Network Operators will be also the IoT Service Provider.

The security services provided by Network Operators can provide a critical role in securing the assets used to provide an IoT Service. These can include:

- IoT Service data being sent between an IoT Endpoint device and the IoT Service Platform – this includes both primary privacy-sensitive data (e.g. end user related data) and commercially exploitable data (e.g. such as actuator control data) which may also have some secondary privacy impact.
- The security assets (IMSI, keysets etc.) and network configuration settings (APN, timer values etc.) used within Endpoint devices (including Gateway devices).
- IoT Service Provider's business-sensitive information, including brand reputation, customer/user data under company responsibility, strategic information, financial data, health records, etc.
- An IoT Service Provider's business infrastructures, service platforms, corporate networks and other private network elements.
- Public (i.e. shared) datacentre infrastructures provided by the Network Operator that are used by the IoT Service. This can include public services, hosted capabilities, virtualization infrastructures, cloud facilities, etc.
- Communications network infrastructure, including radio access networks, core network, backbone networks, basic service functions (DNS, BGP, etc.), access to and aggregation of fixed and cellular networks, etc.

3 Network Security Principles

Proper and reliable security mechanisms must be implemented by Network Operators in their networks.

In this section it is described how networks can provide value within the IoT ecosystem.

The most fundamental security mechanisms provided by a communication network are:

- Identification and authentication of the entities involved in the IoT Service (i.e. Gateways, Endpoint devices, home network, roaming networks, service platforms).
- Access control to the different entities that need to be connected to create the IoT Service.
- Data protection in order to guarantee the security (confidentiality, integrity, availability, authenticity) and privacy of the information carried by the network for the IoT Service.
- Processes and mechanisms to guarantee availability of network resources and protect them against attack (for example by deploying appropriate firewall, intrusion prevention and data filtering technologies)

3.1 Secure Identification of Users, Applications, Endpoint Devices, Networks and Service Platforms.

Identification consists of providing unique identifiers to the entities within the IoT Service, and correlating these electronic identities to real-world, legally-binding identities.

Within a cellular connected IoT Service, Endpoint devices are identified using IMSI and/or IMEI (EIDs may also be used for devices with eUICCs). Networks are identified using network codes and country codes. Each method of providing identity has varying levels of secure assurance associated with it.

Identity plays a crucial role in the process of authentication as secure authentication can only be achieved on the basis of a secure identity. It is therefore essential that the identities (for example an IMSI, IMEI or ICCID) issued and used within an IoT Service are securely protected against unauthorised modification, impersonation or theft.

One practical problem an IoT Service Provider may face is that their IoT Service may require communications with many IoT Service Platforms, each of which may require a separate unique identification. Each identity used to establish a communications link to each IoT Service Platform will then need to be securely provisioned, stored and managed by the IoT Service.

Where appropriate for the IoT Service, Network Operators recommend the use of UICC based mechanisms to securely identify Endpoint devices. Network Operators can also extend the secure storage functionality provided by the UICC to the IoT Service Provider to enable them to store additional IoT Service related identities on the UICC. This technique can be applied to both cellular and non-cellular Endpoint devices (e.g. EAP-AKA [27]).

“Single sign-on” services could also be provided by Network Operators to allow Endpoint devices to establish and prove their identity once, and then connect to several IoT Service Platforms without further inconvenience. The security trade-offs and risks of using such a service must be considered across the multiple platforms.

3.2 Secure Authentication of Users, Applications, Endpoint Devices, Networks and Service Platforms.

According to NIST [10], “authentication” is “verifying the identity of a user, process, or Endpoint device, often as a prerequisite to allowing access to resources in an information system”.

Network Operators can provide services to ensure that the users, applications, Endpoint devices, networks and service platforms associated with an IoT Service are securely authenticated.

Authentication has a related property – that of non-repudiation. According to NIST [10], a definition of non-repudiation is: “assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information”. Non-repudiation, depends on asserting that authenticity has not been violated when identifying the source of that transaction or message.

3.3 Provide Secure Communication Channels

Network Operators provide communications security mechanisms for wide area cellular and fixed networks providing the reassurance of “best-in-class” communications integrity, confidentiality and authenticity. Where appropriate, Network Operators can provide and manage secure connections to enterprise networks using Virtual Private Networks (VPNs) and encrypted internet connections.

The purpose of a secure communication channel is to ensure that the data being sent over the channel is not processed, used or transmitted without the knowledge and consent of the data subject. Encryption technologies play a crucial role in secure data transmission by assuring the properties of confidentiality, integrity and authenticity. Encryption must be appropriate to the system being designed and deployed taking into account Lightweight Endpoint devices, network aspects (such as satellite backhaul constraints) and the service being provided.

Network Operators can provide IoT Service Providers with data encryption services to ensure communication integrity and network resilience.

Network Operators traditionally provide public telecommunications infrastructure or a mixture of public or private network infrastructure. Many Network Operators can ensure that the customer/user data that transits their public network infrastructure is encrypted between the point that the data enters the public network infrastructure to the point that it leaves the network. Where required, Network Operators can also assist IoT Service Providers to deploy or derive their own encryption credentials to ensure confidentiality of IoT data during transit through the Network Operator’s infrastructure.

Network Operators can provide their customers with private networks where dedicated communication channels are provided for the use of a single customer to ensure that no data traverses a public network such as the Internet. Such private networks could be created:

1. By using a tunnelling protocol such as Layer Two Tunnelling Protocol (L2TP) and secured using protocols such as Internet Protocol Security (IPsec), or
2. By creating a dedicated network for the IoT Service by deploying a separate instance of the core network with shared radio network – as per the example shown below.

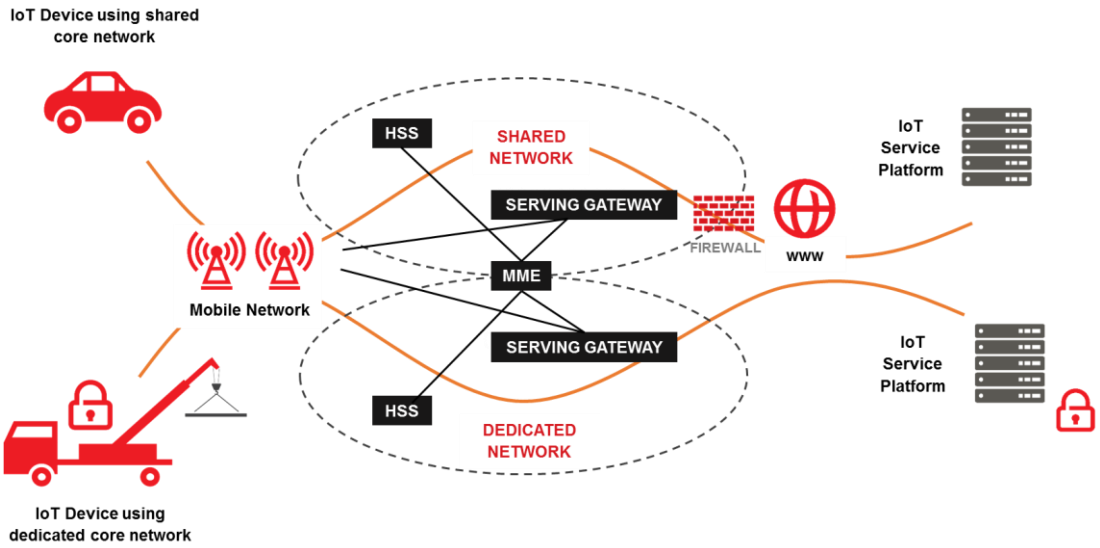

Figure 2 - Example of Private Network Configuration

3.4 Ensure Availability of Communication Channels

According to NIST [10], “availability” is the property of being accessible and useable upon demand by an authorized entity.

Network Operators can provide IoT Service Providers with available networks. The most fundamental mechanisms provided by Network Operators to provide network availability are as follows:

3.4.1 Use of Licenced Spectrum

GSMA Network Operator members will operate networks using dedicated licenced spectrum under the terms of the licences issued by their national regulators. Use of licensed spectrum ensures interference from other radio technologies is kept to a minimum as any unauthorised use of this spectrum will be subject to prosecution. Network operators together with national regulators will seek out any unauthorised sources of interference to ensure network availability is not impacted.

Use of licenced spectrum, which provides the Network Operator with dedicated radio bands in which to operate their network, ensures that careful network coverage and capacity planning can be undertaken by the Network Operator to ensure maximum network availability to their customers.

3.4.2 Implementation of Standardised and Proven Network Technologies

GSMA’s Network Operator members implement standardised network technologies such as GSM, UMTS and LTE as specified by standards bodies such as the 3GPP. The use of standardised technologies not only assures interoperability between Network Operators, it

also ensures the standard is subject to maximum scrutiny during its creation to ensure the robustness of its technology.

3.4.3 Implementation of Tested and Certified Network Technologies

Many parts of a Network Operator's network will be tested and certified according to international test standards. Complex Endpoint devices and the communication modules they contain will be subject to 3GPP test specifications [13] via GCF, PTCRB and Network Operator acceptance testing. Radio Access Networks (RAN) will be subject to 3GPP test specifications [14] via Network Operator acceptance testing. UICCs will be subject to 3GPP test specifications [15] via Network Operator acceptance testing and, additionally, may be subject to GSMA SAS certification [16].

3.4.4 Resilient Network Topographies and Configuration

Network Operators provide resilient networks implementing and building in the necessary geographic redundancy and isolation to ensure maximum availability with minimum downtime. All network elements are carefully configured and monitored to ensure strict quality of service and service level agreements are met.

3.4.5 Real Time Monitoring and Management of Network Resources

Network Operators implement state of the art network operations centres that monitor the performance of their networks on a 24/7 basis and in real time to manage network traffic, respond to network demand and fix faults. Additional information can be found in section 4.10

3.4.6 Threat Management and Information Sharing

The GSMA's Fraud and Security Group (FASG) provides an open, receptive and trusted environment for all Network Operators to share fraud and security intelligence and incident details in a timely and responsible way. The group assesses the global fraud and security threat landscape, analyses the associated risks for Network Operators and their customers and defines and prioritizes appropriate mitigating actions.

3.4.7 Roaming Services

Due to the use of standardised network and Endpoint device technologies and interconnect services, Network Operators can offer network roaming services, further enhancing network coverage and availability for their customers.

3.4.8 Endpoint Device Performance Monitoring and Management

Network operators can measure the performance of the Endpoint devices that connect to their networks to isolate Endpoint devices that may be creating excessive amounts of radio interference (e.g. do not conform to national regulations) or network signalling traffic (e.g. do not conform with GSMA Connection Efficiency Guidelines [17]) which, in turn, may be degrading the performance of the overall network. Endpoint devices can thus be monitored, disconnected or their firmware may be updated when abnormal behaviour is detected.

4 Privacy Considerations

To realise the opportunities that the IoT offers, it is important that consumers trust the IoT Service Providers who are delivering IoT Services and collecting data about them. The GSMA and its members believe that consumer confidence and trust can only be fully achieved when users feel their privacy is appropriately respected and protected.

There are already well-established data protection and privacy laws around the world which have been applied, and complied with, by Network Operators. Operators believe that it is possible to apply existing data protection regulations and principles to address privacy needs in the context of IoT Services and technologies.

However, IoT Services typically involve operators working together with IoT Service Provider partners. It is important that there is regulatory clarity and legal certainty around IoT Services and that privacy and data protection regulations apply consistently across all IoT Service Providers in a service and technology-neutral way.

Network operators should be aware that if they process data in any way they need to sign a Data Processing Agreement (DPA) with the IoT Service Provider. The data protection and security practices developed for a given IoT Service should reflect the overall risk to an individual's privacy and the context in which data about the individual is collected, distributed and used. Any regulatory interventions should be limited to areas where identified risks emerge and existing measures are insufficient to address these.

Network operators can draw on their extensive experience in addressing privacy and security issues and work collaboratively with IoT Service Providers, to embed privacy and security into IoT technologies and the overall consumer experience. Such collaboration will ensure IoT Service Providers are able to identify and mitigate the relevant consumer privacy risks in the context of the service being delivered.

For more information please see the GSMA Mobile Privacy Principles:
http://www.gsma.com/publicpolicy/mobile-and-privacy/mobile-privacy-principles

5 Services Provided by Network Operators

Network Operators can provide IoT Service Providers with secure cellular and fixed wide area networks (WANs).

This section contains best-practice recommendations when connecting IoT Services to wide area networks. Where appropriate, the recommendations will be independent of the technology used, but will also use best practice from cellular and other network types.

5.1 Secure Subscription Management Procedures

This section contains recommendations on how IoT Service Provider subscriptions should be managed by Network Operators:

- The Network Operator or IoT Service Provider should perform an assessment of the network services that are needed to enable the IoT Service (voice, data, SMS, etc.) both now and in the future.

- Based upon this assessment the Network Operator should operate on the “principle of least privilege” and provision the IoT Service Provider’s subscriptions with only those services required for the specific IoT Service. For example:
    - IoT Services that only use data bearers should not be provisioned with voice and SMS services.
    - Where an Endpoint device only connects to a known IoT Service Platform, the subscription associated with the device should only allow connection to a known whitelist of IP address ranges (or domains).
    - If the IoT Service uses voice or SMS, the use of a preconfigured fixed dialling list should be considered.

- Network Operators should implement secure subscription management processes for IoT subscriptions that enable critical IoT Services (for example for the subscriptions associated to critical healthcare services). These services should not arbitrarily be disconnected.
- Network Operators should identify the UICCs used for IoT Services from traditional UICCs used to provide traditional services and, if required by the IoT Service Provider, segregate these appropriately.
    - If the UICCs used for IoT Services are segregated from the UICCs used for traditional “handsets” then this provides a basis for more secure and efficient management of the associated subscriptions by the Network Operator than might otherwise be the case. For example, a Network Operator might consider using a separate HLR/HSS for Endpoint devices which have extended lifetime and is better configured to support these UICCs for a very long period of time (i.e. many years).

5.1.1 UICC Supply and Management

5.1.1.1 Remote management of the UICC (Over-The-Air, OTA)

IoT Endpoint devices are not physically accessible in some scenarios. To be able to perform changes to the UICC remotely, UICC OTA management should be supported by the Network Operator. The UICC OTA security mechanisms should follow the latest ETSI [1] [2] and 3GPP [3] specifications and use the most appropriate level of security for the IoT Service.

IoT Endpoint devices should support the necessary APDU commands recognized by the UICC to make sure that UICC OTA command execution will succeed.

5.1.1.2 Non-Removable UICC

The Network Operator should provide non-removable UICCs (i.e. Machine Form Factor) for IoT Services where the service threat model suggests that the IoT Endpoint device may be vulnerable to physical tampering. Additional security measures should be applied to be able to detect and react to such a threat.

5.1.1.3 Remote Management of Embedded UICCs (eUICCs)

The Network Operator should provide secure remote management of non-removable UICCs (i.e. eUICCs) for IoT Services which require Endpoint devices to be located in remote or difficult to reach locations.

For example, for IoT Service Providers who need to manage a large number of eUICCs that are embedded into Endpoint devices for which the IoT Service Provider is not the owner and cannot easily access (e.g. a car).

Typically Operators use IoT Connectivity Management Platforms to monitor and control the communication services offered to the IOT Devices by (e)UICCs.

The Network Operator should support the GSMA's Remote Provisioning Architecture for Embedded UICC Technical Specification [7].

5.1.1.4 UICC-based Services

A Network Operator might provide an IoT Service Provider with UICC based services. This makes it possible for the IoT Service Provider to use the UICC as a secure and tamper resistant platform for their IoT Services. Such UICC-based services are usually developed in JavaCard™ and are interoperable between all JavaCard™ compliant UICC cards. An example of such an application for an IoT Endpoint device could be the monitoring and reporting of the network quality. The tamper resistance feature provided by the UICC platform is highly valuable for IoT Endpoint devices that can be physically accessed by attackers. Leveraging the UICC as a common secure element for all stakeholders may also make secure IoT Endpoint devices more cost effective.

The UICC may also be used for tamper-resistant storage of sensitive data for IoT Services, including security keys controlled by the IoT Service Provider. ETSI TS 102 225 [1] leverages on the Confidential Card Content Management feature of the Global Platform Card Specification to enable IoT Service Providers to independently manage their own security domain on a UICC.

An IoT Service Provider or Network Operator can ask the UICC Supplier to create such security domains inside the UICC. The issuer of the UICC should ensure that it is protected by proper security keys and the IoT Endpoint device can execute the necessary APDU commands to access it.

Additionally the UICC could also be used to encrypt (using its securely stored keys) and send sensitive content for IoT Services, or provide security services for Endpoint device based applications via services such as the Open Mobile API [4].

5.1.1.5 Secure UICC Manufacturing and Provisioning

A Network Operator should source their UICCs from manufacturers whose manufacturing and provisioning processes are accredited according to the GSMA's Security Accreditation Scheme (SAS) [16].

5.2 Network Authentication and Encryption Algorithms

This section contains recommendations and best practices for network authentication and link encryption for different wide area networks.

The Network Operator should implement network authentication algorithms that meet the lifetime expectations of the IoT Service Provider's Endpoint devices.

Network Operators provide several types of communication services that can be used by an IoT Service, such as USSD, SMS and IP data connectivity. For the purpose of this document only IP data connectivity is discussed since it is the most utilised form of communication service used by IoT Services.

USSD and SMS are used by many existing IoT Services so it is worth highlighting that USSD and SMS have limited security support capabilities in comparison to IP data connectivity. In general, USSD and SMS traffic is not by default 'end to end' cryptographically protected by the Network Operator and cryptographic protection mechanisms to ensure confidentiality and integrity are not available for SMS messages. IoT Service Providers that use USSD or SMS for their communication need to be aware of the vulnerabilities associated with USSD and SMS and, where possible, implement additional encryption at the service layer.

5.2.1 Security of GSM/GPRS (2G) Systems

Network Operators who provide GSM/GPRS networks should:

- Use a minimum of 128 bit A5/3 stream cipher to protect link between the IoT Endpoint device and the base station. Network Operators should avoid A5/1 and A5/2 or use of unencrypted links where possible.
- Use the MILENAGE authentication algorithm. Network Operators should avoid COMP128-1 and COMP128-2. Network Operators should consider support of the TUAK authentication algorithm
- Take appropriate measures to address and mitigate false base station attacks.

In GSM/GPRS systems the network is not authenticated by the Endpoint device, only the device is authenticated by the network. End-to-end encryption at the service layer is therefore recommended when using GSM/GPRS systems. Consideration must be given to practical processing, Endpoint device limitations and network bandwidth constraints in solutions provided as IoT Services.

In GSM/GPRS systems the GTP-tunnel between SGSN and GGSN which is created over the GRX-network is not encrypted. The Network Operator should ensure the security of this link by ensuring GRX-network is managed as a private network.

5.2.2 Security of UMTS (3G) Systems

UMTS networks allow for mutual authentication, where the Endpoint device is not only authenticated by the network, but the network is also authenticated by the device.

Network Operators who provide UMTS networks shall support the MILENAGE authentication and key generation algorithm. Network Operators should support the Kasumi confidentiality and integrity encryption algorithms.

Network Operators should consider support of the TUAK authentication algorithm

5.2.3 Security of LTE (4G) Systems

Network Operators who provide LTE network shall support the MILENAGE authentication algorithm. Network Operators should support the LTE EEA1, EEA2 or EEA3 encryption algorithms.

Network Operators should consider support of the TUAK authentication algorithm.

Network Operators are advised to review the GSMA whitepaper “Wireless Security in LTE Networks” [30].

5.2.4 Security of Low Power Wide Area Networks

Several Low Power Wide Area Network (LPWAN) technologies exist with most being proprietary and often not in the public domain. Examples include LoRa, SigFox and Weightless.

While LPWAN technologies were initially developed to be “standalone” many of these technologies are now being considered by 3GPP for inclusion within the 3GPP standards.

As such, security guidelines related to Low Power Wide Area Networks are out of the scope of this document. .

5.3 Security of Fixed Networks

Recommendations for default configuration of Wi-Fi networks where under the control of a Network Operator or an IoT Service Provider include EAP-SIM [28] or EAP-AKA [27] authentication and may rely on the UICC EAP framework of ETSI TS 102 310 [8].

5.4 Traffic Prioritisation

Network Operators can provide Quality of Service levels appropriate to the IoT Service being provided.

5.5 Backhaul security

The 3GPP standards that specify GSM, UMTS and LTE do not mandate the use of encrypted backhaul links. Moreover, RAN and backhaul sharing between different Network Operators may introduce additional security vulnerabilities.

The Network Operator should implement backhaul encryption for GSM, UMTS and LTE networks for both end user data and signalling plane data traffic.

5.6 Roaming

Network Operators can provide IoT Service Providers with an international mobile footprint through use of roaming services.

Roaming networks can be vulnerable to security breaches due to the relative openness of the SS7/Diameter interworking functions used to connect the home and roaming networks. This is of particular relevance to IoT Services due to the potentially high proportion of IoT Endpoint devices that will reside on roaming networks. There are a few reasons for the high

percentage of roaming Endpoint devices. Firstly, many Endpoint devices are manufactured in one location and distributed globally. Therefore in many cases replacing a UICC is not practical or not possible in the case of embedded UICC. Secondly, in many cases the roaming status is preferable over local connectivity, due to the potential multiple coverage by several roaming networks. The formation of global alliances with a global UICCs and dedicated IoT roaming agreements facilitate the permanent roaming situation where allowed by local legislation.

Network Operators should consider how to protect their HLRs and VLRs against Denial of Service attacks (including unintentional DoS attacks), requests from unauthorised sources and exploitation of “steering of roaming” services.

The roaming is facilitated by the inter-Network Operator signalling protocols that are exchanged between the main core mobile network entities:

1. Between the VLR or the SGSN in the roaming (visited) network and the HLR at the home network – the MAP (Mobile Application Part) protocol (for CDMA networks, IS41 is similar to MAP).
2. Between the MME in the LTE roaming network and the HSS at the home LTE network – the Diameter (certain variants such as S6a) protocol.
3. Between the SGSN/S-GW in the visited network and GGSN/P-GW at the home network – the roaming data transfer using GTP (GPRS Tunnelling Protocol).

This section will concentrate on roaming security issues related to IoT Services. General roaming security issues are covered by the GSMA FASG (Fraud And Security Group) and its sub-groups. Hence, issues such as double registration in roaming, received from two different VLRs located in different countries – a classical roaming fraud scenario – is out of the scope of this document.

5.6.1 Roaming signalling storms/attacks

IoT has additional security requirements from the mobile network, due to the different nature of the Endpoint devices and the potential high level of service criticality. While serving a large number of Endpoint devices, the mobile network is exposed to signalling storms. An intentionally malicious Denial of Service attack is only one reason for such storms. A power failure, natural disaster or coverage problem in a certain area of a serving mobile network can be common in many countries and therefore cause such issues. All roaming smart meters and other Endpoint devices located in that area will attempt to roam to another roaming network, simultaneously. Such a scenario creates a signalling storm and imposes a severe risk on the home HLR/HSS. 3GPP TS 23.122 [9] defines an Extended Access Barring (EAB) service to address such scenarios: Network Operators can restrict network access to the Endpoint devices configured for EAB, in addition to common and domain-specific access control mechanisms. EAB configuration can be performed in the UICC or in the Endpoint device itself. Network security gateways should be configured to “sinkhole” intentional Denial of Service attacks.

There may also be a need for the home Network Operator (together with the IoT Service Provider) to distinguish between low priority Endpoint devices, and critical Endpoint devices. For example, it may be necessary for healthcare devices to continue to maintain service under signalling storms and service denial attacks. There may be a need for Network to

reject the registration of ‘low priority’ roaming Endpoint devices under signalling storm conditions, but to allow ‘high priority’ Endpoint devices to register. The reject mechanism implemented may be accompanied with a back-off timer, in order to assist the Endpoint device in registration re-attempt, after the signalling storm.

The general recommendation would be for Network Operators to screen all roaming messages received from home networks/roaming partners. In addition to blocking messages from unauthorized/faked home networks/roaming partners, there is a need to filter the messages according to the Endpoint device priority. Under signalling storm/denial of service attacks, there is a need to either allow messages from high priority/critical Endpoint devices, or reject messages from non-critical Endpoint devices. Reject methods are required in order to postpone the registration attempts and other activities for a certain period.

5.6.2 Security-based Steering of Roaming (SoR)

Another security use case that can be carried out by a Network Operator is Steering of Roaming (SoR) of IoT Endpoint devices for security purposes. Rejecting an Update Location without a back-off timer causes the Endpoint device to re-try, and finally to attempt registration from a different roaming (visited) network. Another method for SoR is via OTA, using UICC roaming preferred lists and other parameters stored on the UICC. The UICC’s OTA update capabilities enables the home network to update the preferred roaming lists, which determine the priority of the networks during the selection process of a roaming network. The home network can also refresh the Endpoint device memory with the new list and cause the Endpoint device to search for a new network instantly.

In case a security risk is detected in a specific visited network, the home network may decide to transfer its outbound roaming Endpoint devices to another visited network, using the SoR mechanism. Such an active transfer of Endpoint devices can be made upon the next registration attempt of the Endpoint device, or ad-hoc using the SIM OTA services. A security risk related to a specific visited network can be detected if a problem is reported by a relatively high number of Endpoint devices roaming on that network, or information received by other inputs.

5.6.3 Data Roaming Denial of Service

Denial of Service attacks are not limited to the mobility signalling space, and data roaming is also a potential field for signalling storms. As of today, most of the roaming data is routed from the visited network SGSN (S-GW in case of LTE) to the home network GGSN (P-GW for LTE).The case of LBO (Local Breakout), where the data is routed from the visited network directly to the internet is rarely implemented. The situation in the future might change, due to regulations, such as the EU regulation that enabled the LBO service since July 2014, LTE and especially VoLTE (Voice over LTE), where voice calls made in the roaming network may be handled by the domestic P-GW (such as the case today with regular circuit-switch voice calls made in a visited network).

Signalling storms may happen when the home GGSN/P-GW is flooded with requests for new data sessions. The GPRS protocol creates a secured tunnel between the Endpoint device and the GGSN, and a request for a new session (Create-PDP-Context) results in setting up a tunnel, and allocation of an IP address to the Endpoint device. When IoT Endpoint devices do not behave in a personalised manner, they can generate bursts of requests for new data

sessions as noted before. Denial of Service attacks can be generated by a relatively small number of Endpoint devices, creating multiple requests for new data sessions in parallel. The GGSN/P-GW servers are limited in their capacity and should be protected from such storms.

To prevent signalling storms Network Operators may, based on a security policy, prevent certain devices from connecting to their network by changing the communication profile of the affected devices or by enacting security policies within the network's packet core.

Critical Endpoint devices should receive a service also under denial of service attacks, while the requests of lower priority Endpoint devices are postponed for a certain delay period.

5.7 Endpoint and Gateway Device Management

It should be noted that the hardware and software security measures, including local configuration management consoles for Endpoint devices and Gateway devices are beyond the scope of this document. This section covers network related aspects. See GSMA document "CLP.11 IoT Security Guidelines Overview" [11] for Endpoint device related security guidelines.

5.7.1 Endpoint Device Management

Network Operators can offer IoT Service Providers with basic capabilities to securely configure and manage Endpoint devices and subscriptions, adopting some of the principles and technologies developed for 'traditional' mobile device management. IoT Endpoint devices that use a UICC to register and connect to a cellular network can be managed using the connectivity management platforms, device management platforms and UICC management platforms that exist today.

On top of this basic Endpoint device management capability more complex and specific Endpoint Device management functionality can be provided by the IoT Service Platform.

An example of a typical Endpoint device management architecture is shown below and is taken from the ETSI M2M communication principles [19].

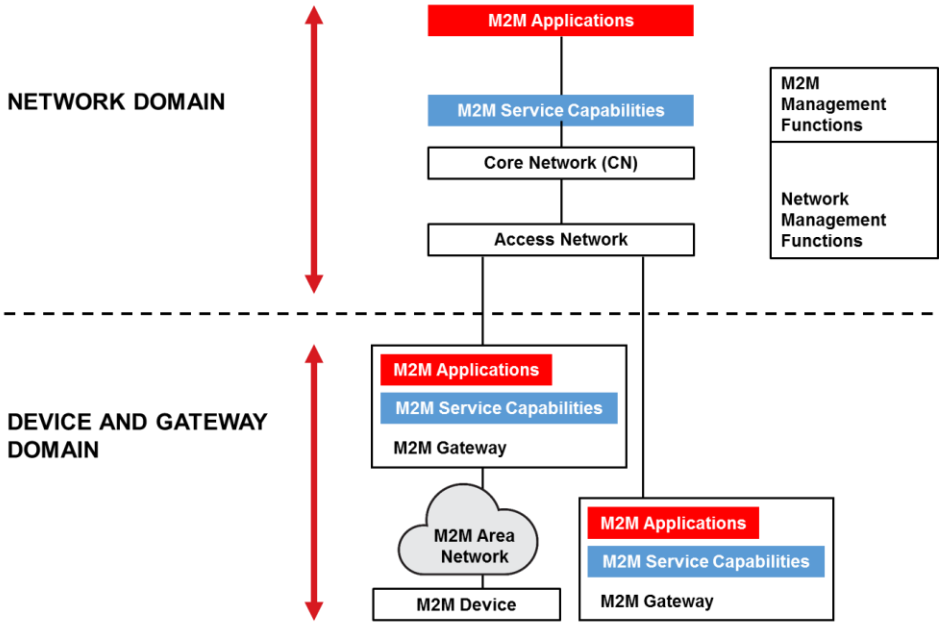

Figure 3 - ETSI High Level Architecture for M2M Device Management

The blue blocks indicate what is traditionally managed by the Network Operator's existing device management platforms and the red blocks indicate the service component that are managed by the IoT Service Platform.

Network operators can undertake some of the device management functions indicated in red at the request of the IoT Service Provider.

5.7.2 Management of Gateway Devices

The use of Gateway devices potentially introduces one more level of device management complexity to the IoT Service Provider. In some cases the IoT Gateway device may be a UICC based device which connects to a cellular network, in some other cases fixed lines are used.

The Gateway should be a managed object, in order for it to be monitored and updated with new firmware or software should the need arise. Protocols for providing secure firmware and software updates and secure software and systems integration mechanisms should be used to secure the interconnection of the Gateway to the network backbone.

Network Operators can provide and manage secure Gateways on behalf of the IoT Service Provider which allow Endpoint devices to securely connect in a way that best integrates with the Network Operator's wide area network security mechanisms.

Gateways that connect using fixed network connectivity can be managed remotely using the Broadband Forum TR-069 Customer Premises Equipment (CPE) Wide Area Network (WAN) Management Protocol [20].

Gateways that connect using cellular network connectivity can be managed remotely using the OMA Device Management (DM) and Firmware Update Management Object (FUMO) protocols [5] [6].

5.7.3 IoT Endpoint Device Blacklisting

Network Operators should implement IoT Endpoint device blacklisting and connection to the GSMA Central Equipment Identity Register (CEIR) database. The CEIR is a central database, administered by the GSMA, containing IMEIs associated with lost and stolen Endpoint devices and devices that should not be granted network access. Once an IMEI is entered into the CEIR the Endpoint device containing the IMEI will be blacklisted by all Network Operators who take that data and implement local blacklisting based on their use of equipment identity registers (EIRs).

Network Operators may also implement localised device “greylisting” to allow the temporary suspension of ‘suspect’ devices whilst the Network Operator investigates the nature of such devices prior to any blacklisting. It should be noted that for critical services such as healthcare, blocking an IMEI may not be desirable or possible. It is important that the details of connected Endpoint devices should be clearly understood by Network Operators in so far that the true application (or host) of an Endpoint device can be discerned. Endpoint devices that leverage the IMEI issued to a communications module vendor should support Device Host Identify Reporting which is a capability that enables the Endpoint device to report host information to the Network Operator. Device Host Identify Reporting is described in the GSMA’s Connection Efficiency Guidelines [17].

5.8 Other Security Related Services

5.8.1 Cloud Services / Data Management

Network Operators can supply customers with hosted cloud IoT Service Platforms for implementing IoT Services and also provide services for storing and managing the data produced by such services.

Network Operators can supply either a private cloud or a shared cloud infrastructure depending upon the requirements of the IoT Service Provider.

5.8.2 Analytics-based Security

Network Operators can provide data analytics and deep packet inspection services to identify threats and anomalies in the data generated by IoT Services. An example could be that a Network Operator could periodically perform deep packet inspection for specific strings like social security numbers and GPS coordinates that might suggest that such information is not protected properly and alert the IoT Service Provider responsible that information could be leaking.

This is advantageous for IoT because Lightweight Endpoint devices and services cannot provide this functionality themselves. Network Operators can provide IoT Service Providers with visibility of the security status, identified threats and attacks as well as an overall security health check. These introspection services are vital to ensure that threats are not infiltrated “inside the pipe”, particularly where data services are encrypted. Services provided include:

- Use of anomaly detection and machine learning to spot problems.
- Build intrusion protection systems into real-time Endpoint device diagnostics.
- Provide dashboard for visualising and easily identifying anomalies.

- Provide automated means for flagging and blocking suspicious connections.
- Provide threat analysis of cloud based services.

5.8.3 Secure Network Management

Network Operators can provide networks that are securely managed and maintained.

- Backup channels in case of physical or logical link failure
- Identify link failure as evidence of potential security breach
- Implement roaming policies impacting security and integrity
- UICC/SIM Management
- Management of secure information
- Membership of CERTs and participation in threat information sharing to mitigate and prevent future attacks.
- Protection against Denial of Service attacks
- Carry out periodic security scans / vulnerability assessments
- Management and handling of network security related regulatory requirements
- Restrict communications options to the strict minimum required for a given IoT Service.

5.8.4 Secure IoT Connectivity Management Platform

Network Operators are increasingly making use of dedicated core network and OSS infrastructure to manage IoT subscriptions and price plans in an efficient and scalable manner. Access to such infrastructure is often exposed to the operator's business customer (i.e. an IoT Service Provider) so they can self-manage their subscriptions (that would include activation of the service, suspension, etc…individually or in bulk).

The service platform guidelines offered in CLP 12 "IoT Security Guidelines for IoT Service Ecosystem" [26] offers valuable guidance that can benefit the Network Operator who support IoT Connectivity Management Platforms. These guidelines contain the following recommendations:

- Network Operators should make sure access to their IoT Connectivity Management Platform's web portal, which could be Network Operator or Cloud hosted, uses 'best in class' encryption as per the most recently published industry guidance from organisations such as NIST [24] and ECRYPT2 [25].
- Network Operators should make sure access to their IoT Connectivity Management Platform's web portal makes use of standard "best practice" procedures for password creation, updating and resetting.

5.8.5 Certificate Management

Network Operators can provide X.509 certificate management services.

5.8.6 Multi Factor Authentication

Multi factor authentication services typically require a user to authenticate themselves using an electronic token in addition to a username and password. As such, multi factor authentication can provide additional protection against access to IoT Services from unauthorized users.

The GSMA's Mobile Connect initiative [12], together with OpenID Connect [21], FIDO [22] and ETSI MSS [23] are examples of multi factor authentication enablers that can enable an IoT Service Provider to obtain additional authentication and information from their end users. The end user in this context being a human that can provide information to an IoT Service Platform to provide different levels of assurance – examples include entering a PIN and providing a biometric signature.

Whilst most multi factor authentication solutions are currently used to enable traditional "smartphone" services such technologies could be applied to IoT Services that require the assurance of human authorisation for certain tasks such as performing a network attach operation, software update or hard reset.

For example, using multi factor authentication, a mobile identity could be used in addition to a Gateway device inside a connected car. In this use case the multi factor authentication infrastructure could act as an additional authorization layer for the car's occupants to gain access to infotainment and payment services provided within the car.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	08-Feb-2016	New PRD CLP.14	PSMC	Ian Smith GSMA
1.1	17-Nov-2016	References to GSMA IoT Security Assessment scheme added. Minor Editorial corrections.	PSMC	Ian Smith GSMA

A.2 Other Information

Type	Description
Document Owner	Internet of Things Programme
Contact	Ian Smith - GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.