Connected
Living

Embedded Mobile Guidelines

Version 3
March 2012

Embedded Mobile

Whitepaper Embedded Mobile Guidelines

Release 3

28 March 2012

.

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

Copyright Notice

Antitrust Notice

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

Table of Contents

List of Tables

List of Figures

1 Document Purpose

Embedded Mobile (EM) refers to a family of devices and services that use wide-area mobile network technologies to enable communications between machines themselves and also with humans. The genesis of this initiative stems from a GSMA objective to explore new market opportunities for the mobile industry beyond traditional handset and PC data card hardware.

The goal of this document is to establish cross-industry guidelines for the design and development of emerging EM devices, applications and Wide Area Network (WAN) considerations. This will drive consensus around common module and implementation rules to drive economies of scale, and encourage the development of new applications and services for the end-users based on wireless Wide Area Network (WWAN) connectivity.

1.1 The Embedded Mobile (EM) Initiative

The GSMA EM initiative is a market development programme designed to accelerate the usage of wireless connectivity by a wide range of devices across the education, healthcare, automotive and utilities sectors. In most cases, a wireless modem will be embedded into the device. The short-term goal is to trigger market expansion to achieve 500 million connected EM devices by 2013.

The GSMA is supported by some of the world’s leading mobile operators, and is focused on identifying and lowering the main barriers for each of the key sectors and bringing embedded devices to market via appropriate, simple and streamlined processes. Some of the objectives are common across the sectors; for example, helping to bring costs down through economies of scale by introducing common design guidelines for new embedded modules, such as those contained within this document, and stimulating and participating in regulatory discussions.

1.2 Intended Use of the Guidelines

These guidelines are targeted at a wide stakeholder audience in the EM ecosystem.

This document is intended to capture current views and implementation guidelines for EM applications from a diverse group of companies in the mobile eco-system. The document also suggests potential design improvements with the aim of lowering deployment and operational management costs.

The guideline document is intended to be used by mobile network operators (MNOs), vendors and companies from outside the mobile eco-system that are interested in adding mobility to their device and service offerings. The guidelines will evolve as additional design information, new technologies and new usage scenarios are considered; these evolutions will be captured in subsequent revisions of this document.

The process of developing this document has facilitated cross-stakeholder discussions about saving costs and simpler implementation solutions.

2 Executive Summary

Release 3.0 of the Embedded Guidelines document remains consistent with earlier releases 1.0 and 2.0 by addressing the three main market development goals set out for the GSMA's EM program. These are:

- Reduce fragmentation in the EM market
- Increase volumes and economies of scale
- Drive cross–industry awareness of module designs that contribute to scale economies

In developing each release of the Embedded Guidelines, the GSMA established a working group to develop cross-industry consensus around a family of low-cost embedded modules and also a set of guidelines to achieve cost and time savings in hardware and service implementation activities. The GSMA facilitated industry workshops which attracted a high level of participation internationally and from over 25 companies across the mobile eco-system.

Through extensive deliberations, four basic module types have been proposed based on various combinations of low/high application complexity and low/high bandwidth network technologies.

		Application Complexity	
		Low	High
Host Network Attributes	low bandwidth	Module Type A	Module Type B
	high bandwidth	Module Type C	Module Type D

Table 1: Module Type Categorisation

The choice of network technology signals the importance of host network attributes; in countries such as South Korea, Japan and Australia, even low complexity and low bandwidth applications need to be supported with 3G solutions due to the retirement of 2G networks. The application complexity dimension distinguishes basic connectivity and relatively low data volume solutions from those that require more complex processing and/or higher data rate capabilities.

The guidelines provide guidance on technical design and operational issues, such as embedded module design, radio interface, remote management, UICC provisioning and authentication. These are intended to reduce the cost of developing and deploying EM solutions. The guidelines also include a cost driver checklist that device manufacturers, technology providers and MNOs can use to assess design trade-offs.

In addition to guidelines for the basic family of embedded modules, this document addresses sector-specific use-case needs in each of the following priority verticals:

- Automotive / Transport
- Consumer electronics, including education,

- m-Health
- Utilities

Release 3.0 of the Embedded Mobile Guidelines, published in March 2012, builds upon earlier releases by adding or updating content in the areas of application programming interfaces (APIs), network management aspects, and in each of the priority vertical sectors.

3 Introduction

This document is one of the outputs of the GSMA EM programme. Its objective is to address the fragmentation and insufficient economies of scale in the cost of modules, as well as complexity of integrating and deploying EM solutions. Reducing fragmentation will help to grow the volume of network connected devices and user-driven applications. Another objective of these guidelines is to educate the industry about various processes (provisioning, certification, business model), and to guide companies as to the compromises between cost and feature sets.

Achieving these objectives involved a series of cross-industry discussions and workshops. These discussions led to the development of market guidelines on the family of basic module types, recommendations on design and implementation for embedded mobile devices, and proposals for changes in industry operating models to encourage re-use and lower-costs.

This document focuses on the design and deployment issues that will enable the EM market over the next 1-3 years. The structure of the document is as follows:

General Guidelines For Embedding Module Design

Service Layer and Application Programming Interfaces (APIs)

Guidelines for Provisioning and Management

Guidelines for Testing and Certification

Guidelines for Security and Fraud Risk Management

Guidelines for Network Aspects

Guidelines for Roaming

Service Quality And Availability

Specific Guidelines For Key Vertical Sectors

Annexes: Further Use Cases

The wide and international level of participation in developing and maintaining these guidelines shows the industry commitment to join forces to deliver a standardized approach to develop cost effective and up to date modules, devices and services.

3.1 Approach Taken for the Discussion of Embedded Mobile Guidelines

The Embedded Mobile Guidelines focus on the fragmentation issues around embedded modules and define a family of general module types that are intended to reduce market uncertainty, drive critical mass and promote economies of scale.

The document also contains guidelines for a range of technical design choices. This discussion was also extended to certification, provisioning and security issues for the basic family of modules, as well as service layer, roaming and network management aspects.

The following list of vertical segments was also considered in the discussion process.

- Automotive / Transport
- Consumer electronics, including education
- m-Health
- Utilities

These application segments are not exhaustive and were selected on the basis of priorities expressed in the GSMA programme. Many other categories could follow, including but not limited to such vertical sectors as:

- Street furniture (for example. electronic road signs/traffic lights/street lights)
- Security (for example. Closed Circuit Television (CCTV), Asset tracking, alarms)
- Industrial control systems (for example. machine time management; lifts; air conditioning controls)

3.2 Reading Guide

Throughout this document, the following convention is used for points of discussion:

High Level Requirement — A short statement of the needs from the point of view of one or more of the stakeholders/ecosystem players based on identified usage scenarios (use cases).

Considerations — The rationale or justification for the requirement and a description of the relevant solutions and options concerning the identified needs, which are available and achievable in the market today.

Guideline — A guideline or recommendation for use in addressing the stated requirement. This guideline uses best practices as a guidance and notes targets for the future development

3.3 Definition of Terms

Term	Description
2.xG	GSM, GPRS, EDGE network technologies.
3G	WCDMA, HSPA and HSPA evolution radio technologies referred to as UTRAN in 3GPP standardization.
LTE	OFDMA based radio access in 3GPP Release 8 referred to as Evolved UTRAN. Further evolution called also LTE-Advanced starting 3GPP Release 10.
Application Service Provider	A party offering a service enabled through the embedded device.
Communication Service Provider or Mobile Network Operator	A mobile network providing the data communication service to an end-user.
Embedded Mobile (EM)	A family of devices and services that use wide-area mobile network technologies to enable communications between machines themselves and also with humans
Embedded Module	The hardware component including its embedded software, which will be integrated into a host device to provide wide area (2G/3G/LTE) radio capabilities.
Embedded Device or Host Device	A device that contains an embedded module.
Embedded Module Vendors	The provider of technology building blocks and complete embedded modules.
Embedded Device Manufacturers	The provider of end-user devices that deliver services using embedded modules.
End-User	A person using the embedded device functionality. This can be both 'private' users (consumer market) and business users. The corporate

	(purchasing) perspective is also considered from this point of view.
UICC	The smartcard used by GSM service providers to securely authenticate users for Embedded Services. The UICC (Universal Integrated Circuit Card) contains the usual authentication applications USIM and/or SIM.
UICC Reader	The hardware component embedded in the embedded device that is providing a slot for inserting a UICC.

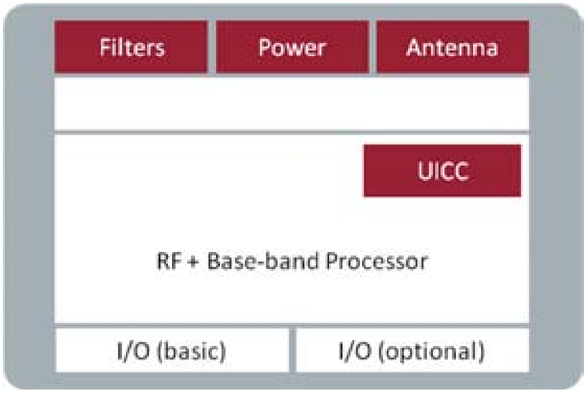
Table 2: Key terms and definitions

3.4 Embedded Module Design Considerations

3.4.1 High Level Module and Embedded System Architecture

This sub-section includes key definitions that will be used in subsequent parts of the document. No guideline is included.

The following exhibit illustrates the architecture for a generalised embedded module. Certain elements, such as the UICC (Universal Integrated Circuit Card) for example, may be integral to the module or be housed off-board; these elements are highlighted in the exhibit. The embedded module itself will be housed in a host device such as a car, vending machine or medical device, for example.



🟥 This is a physical feature of the module that may either be built-into the module or housed off-board on the Host Device

Figure 1: Embedded Module Architecture

The functional components above show the essential physical attributes of an embedded module. The I/O (Input/output) capabilities have been separated into essential and optional blocks to indicate that some module designs may include a range of additional I/O capabilities as determined by a given service application; examples of this are a high-speed serial interface or a camera interface.

Some EM devices may be used only as a modem and not enable embedded applications to run in an application execution environment. Other embedded devices may have enough resources (memory and so on.) to run an application execution environment. An application execution environment may run on a processor embedded in the base band itself, or run on a separate standalone processor. See section 5.3 for additional information on possible EM device configurations.

3.4.1.1 Cost Drivers and Design Considerations

Solution designers can make a number of design choices in specifying the configuration and feature set for a given module type. These choices need to be considered from two perspectives: module-specific costs and total-solution costs.

<u>Module-specific costs</u>

There are three module-specific cost areas that will affect the module design decisions:

- Module hardware costs – costs for the physical components in a module
- NRE (non-recurring engineering) costs – one-time engineering design and licensing fees
- Time to market – costs for additional manpower and an increase in the time to launch a product due to additional approvals activities

Module Features	Details	Impact on Module Hardware per unit Cost	Impact on NRE costs	Impact on time-to-market
RF + Base band	Modes supported	Increases with number of modes	Higher cost due to increased industry, operator and regulatory testing and certification	Higher approval and testing efforts **To avoid time to market delays a detailed certification plan must be developed and executed**
Frequency bands	Bands supported	Increases with number of bands	Higher cost due to increased industry , operator and regulatory testing and certification **Potentially more effort in antenna design depending on the bands used**	Can affect the effort and time to obtain regulatory and MNO approvals, potentially in more than one country
UICC	Location	None	Higher cost for off-board solution	For off-board solution the Embedded device could impact UICC test case compliance and failures and subsequent design changes could result in launch delays
Environ-mental Robustness	Operating Environment	Increases for higher specification components	Increased cost for testing and compliance to higher specifications Failures could impact embedded device design	Failures to meet higher specifications could result in redesign
Shielding		Increases for higher specification components	Higher cost due to design and test for compliance when shielding is required to be provided by host device	Potential delays in time to market when considering challenges in achieving shielding solution
Filters		Increases for higher specification	Increased cost due to design and test for compliance when filtering	Potential delays in time to market when considering challenges

		components	is required to be provided by host device	in achieving filtering solution
Power		Increases for higher specification components	None	n/a
I/O		Increases with number of interfaces	Modules with a low feature set are less costly than full feature products.	None

Table 3: Embedded Module Cost Drivers

3.4.1.2 Total-solution costs

Considerations about the cost effectiveness of an EM service should not focus solely on the embedded module itself. Attention should also be paid to other cost factors including:

- Module integration into the host device
- Embedded device approvals testing
- Deployment and in-service factors.

Some of the main factors that can affect total-solution costs are as follows:

- Production and sales volumes - one time engineering design costs can be significant and need to be amortised over a large number of embedded modules and devices to drive down the per-unit cost.
- Re-use of existing designs - The use of existing designs can provide significant benefits through economies of scale derived from "sunk" costs related to activities such as development and approvals testing.
- Design strategy - device vendors should evaluate the benefits of a "design-in" strategy as distinct from an "add-on" strategy for connectivity. A seemingly low-cost "add-on" solution might be more costly over the product launch phase and also the service life of an embedded device. Furthermore, performance of the embedded device is likely to be superior when shielding, heat dissipation and antenna performance decisions are addressed early in the product development process.

Device hardware costs only constitute a minor part of total costs of ownership. While the cost breakdown will vary depending on individual use cases, the following ranges are calculated based on several specific cases and provide an indication of the cost drivers (as a percentage of the total cost of ownership (TCO) to be considered when making module selection:

- Module hardware: (1%-14%)
- Device hardware and non-recurring engineering costs (NRE (20%-40%) – device development and integration (costs could be higher due to lack of flexibility)
- Certification (1%-2%) – device level versus platform approach
- Support (9%-40%) – provisioning, activation, on-going support and upgrades
- Connectivity and value-added service costs (30%-65%) – based on average revenue per user (ARPU) vs. connections oriented business models
- Value chain complexity / margin stacking

The selection of pre-certified stand-alone modules can have a significant impact on the total cost of ownership for the embedded device developer, as follows:

- Eliminates certification redundancy
- Simplifies and accelerates new product introduction process
- Allows for flexible platforms
- Open APIs (application programming interface) with mature SDK (software development kit) enable module re-use, reduce application development cost, and accelerate time to market
- Volume aggregation provides hardware cost benefits and eliminates a major portion of redundant NRE
- Potential for single SKU (stock keeping unit) for global products simplifies supply chain and logistics

Furthermore, consideration should be given to the potential "end-of-life‟ costs, which can arise from an enforced replacement of devices before the end of their lifecycle; for instance, 2G network decommissioning could trigger additional costs to replace legacy 2G EM equipment. The replacement cost elements that are likely to be incurred include:

- A new 3G communication module (including design and approvals);
- Integration manufacturing, provisioning and service connection;
- Replacement of (part of) the host machine for some vertical sector applications (for example when the communications module is integrated into a device and it is not possible or practical to separately switch out the communications module alone).[1]

The applications with the highest amount of enforced replacement costs within the TCO are those with the longest lifespan (for instance, up to 20 years for smart meters), and those with communications modules that cannot be replaced easily. Therefore, decisions made today on the technologies used in such devices could have implications for the future.

[1] Further analysis of the "end-of-life" TCO costs can be found in the report conducted for GSMA by Analysys Mason: The Total Cost of Ownership for Embedded Mobile Devices, 11 November 2010. Available from connectedlife@gsm.org

4 General Guidelines for Embedded Module Design

This chapter describes the main guidelines for the design of embedded modules and their addition to host devices. There are a multitude of factors to be considered; attention is given to the aspects ranging from the physical integration of components to certification, security and provisioning.

The chapter is structured in three sections:

- Guidelines for embedding the Module into host device
- Guidelines regarding the Radio Interface
- Guidelines regarding the UICC Authentication

Throughout this chapter, the "High Level Requirement – Considerations – Guideline" convention described in the reading guide (section 3.2) is used.

4.1 Guidelines for Embedding the Module into Host Device

4.1.1 Module Types

A key objective of the EM guidelines development process and this document is to address the issue of fragmentation in the machine-to-machine (M2M) industry and lack of widespread implementation knowledge in the broader host-device industry.

Following extensive discussions involving representatives from MNOs and module supplier communities, a broad agreement has been developed regarding the value of promoting four module types. The differences between the module types are captured by two key parameters:

- Application complexity – this dimension distinguishes between EM solutions that entail basic connectivity and relatively low data volumes and those that require more complex processing and/or higher data rate applications.
- Host network attributes – networks in many regions of the world are capable of supporting 2G and 3G applications. In countries such as Japan and South Korea however, 2G networks are either no longer in service or in the process of being phased out. This increases the demand for 3G modules, even for low complexity and low data rate applications.

Based on these dimensions, the following four modules are promoted within this Guidelines document:

		Application Complexity	
		Low	High
Host Network Attributes	Low Bandwidth	Module Type A	Module Type B
	High Bandwidth	Module Type C	Module Type D

Table 4: Module Type Categorisation

In relation to the generalised module architecture, specific minimum features for these module types are listed in the following table.

Features	Type A	Type B	Type C	Type D
GSM	✓	✓	✓	✓
GPRS	✓	✓	✓	✓
EDGE	-	✓	✓	✓
UMTS	-	-	✓	✓
HSDPA/ HSUPA	-	-	optional	✓
LTE			optional	optional
Processing Capabilities	-	Includes an application execution environment	-	Includes an application execution environment
Multi Mode Capability (for example, CDMA)	-	-	Optional	Optional
Hardware interfaces	UART, USB	UART, USB	UART, USB Note: Speed of additional interfaces should be capable of matching 3G speeds	UART, USB Note: Speed of additional interfaces should be capable of matching 3G speeds
UICC	This is an essential component and can be a module-located component or external to the module			

Table 5: Key Embedded Module Type Features

These module categories provide an initial decision support framework for embedded device and application developers to focus on a particular level of functionality and market reach.

The minimum set of attributes for each embedded module type will be augmented as additional features are included depending on end solution needs as discussed below.

4.1.1.1 Other module factors to consider

Certain vertical applications - or customer-specific modules are optimized for a very specific use-case / application. Some examples to consider are listed in the table below, with the detailed requirements addressed in section 12.

	Automotive	Consumer electronics	Healthcare	Smart Metering
Sector-specific considerations	Antenna choice. Specific interface requirements. Impact of host environment on robustness (for example, temperature range)	Size. Power consumption.	Size. Electro-magnetic features. Power consumption. Regulatory approvals.	Impact of host environment. Long life-cycle. Remote management. Regulatory approvals.

Table 6: Additional Module Factor Considerations for Key Verticals

4.1.2 Module Form Factor

4.1.2.1 High Level Requirement

The UICC and embedded module / modem must be physically accommodated within the host device and logically compatible with the host device's architecture and proposed form factor.

4.1.2.2 Considerations

Several integrated solutions are currently in place to achieve the above requirement: Connectorised and/or solderable form factors for traditional M2M applications and consumer electronics devices. There is currently a variety of sizes in the market to meet different requirements. The Peripheral Component Interconnect Special Interest Group (PCI- SIG) has developed a form factor specification named PCI Express Mini CEM (Electromechanical) Specification that is specifically targeted at embedding communications technologies into notebook PCs. The mini-card factor is not limited to notebook PCs but can also be used in other devices. Throughout the remainder of this document, this embedded form-factor will be referred to as the Mini Card. Typically the 3G module will be placed on the Mini Card and the UICC Reader is connected to the card by cabling.

The Mini Card has a small footprint and provides wireless-specific features intended to enable tighter platform integration. The Mini Card specification offers the flexibility to implement solutions based on either PCI Express or USB for the functional data interface to the platform.

4.1.2.3 Guideline

During the design process, the host device manufacturer should consider the design-in of the EM module. Choice of an application and vertical sector will determine the size. Please refer to section 12 (specific guidelines for key vertical sectors) for guidance.

4.1.3 Mounting Concept and PIN Connector Arrangements

4.1.3.1 High Level Requirement

Embedded modules need to be integrated into the host device. The integration means both, the mechanical connection and the electrical connection.

4.1.3.2 Considerations

For the integration of the module it is important to consider the specific device requirements. These requirements can result from the device concept or layout in addition to the designated manufacturing method.

In general there are two types of modules:

a) Connectorised modules with a connector interface and mounting holes or pins
b) Stand-alone module testing modules which are based on Surface Mount Technology (SMT) for automated manufacturing

Connectorised modules can feature for example a board to board connector which connects to a corresponding connector on the device board. The connector is the electrical interface to the device. The antenna interface of the module may be connected separately either to a device’s printed circuit board (PCB) or directly to the antenna of the device. The mechanical fixation of the module can be done through mounting holes or soldering pins.

Surface Mount Technology modules are soldered directly onto the devices PCB. The bottom side of the SMT module is used for soldering. All electrical connections, the antenna as well as the mechanical fixation are done through surface mounting. Optionally, there can be an additional antenna connector for wired antenna connection. Common surface mounting technologies include BGA (Ball Grid Array), castellation interface or LGA (Land Grid Array).

4.1.3.3 Guideline

Choosing between a connectorised module and a Stand-Alone Module Testing (SMT) module featuring Surface Mount Technology (SMT) should take into consideration the following factors:

- Device design: Layout of the application, antenna routing (by way of cable or on the device PCB).
- Manufacturing: Depending on production capabilities for high volume production surface mount technology can offer cost benefits since production can be automated.
- Upgradeability: Connector modules offer the option of exchanging or upgrading modules in existing applications.
- Thermal dissipation constraints: depend on the application and the host environment. Refer to section 4.1.6.
- Test and certification: connectorised (standalone) versus host dependency – cross-check with certification section 7.3.

4.1.4 Hardware Interfaces

4.1.4.1 High Level Requirement

The use of hardware interfaces on embedded modules is either required or optional depending on a vertical application.

4.1.4.2 Considerations

Major interfaces requirements deployed in embedded modules are described below.

In the mini-card variant of the identified four module types, certain interfaces are not supported on a connector. The supported interfaces include: power, UICC, antenna, I2C, Inter-Integrated Circuit UART (Universal Asynchronous Receiver/Transmitter), functionality is offered through USB interface.

Power Interface

A power supply interface is mandatory for all modules. The range of the supported power supply varies between 3.0V-4.5V and is implementation specific. The module may also have power supply interface for the Real Time Clock (RTC).

UART (Universal Asynchronous Receiver/Transmitter) Interface

UART interface is mainly used for the communication or a debugging function of the module. The UART interface is mandatory for all modules. The baud (unit of transmission speed) rate supported by the module ranges from 1200bps to 115200bps. For the Type C/D module, it should support the baud rate of at least 4Mbps.

Embedded modules are designed as DCE (Data Communication Equipment), and must have at least one UART interface to support DCE-DTE (Data Terminal Equipment) connection. Typically UART interfaces have two ports:

1. RXD – The Receive port of UART, by which embedded modules receive data from the client (DTE)
2. TXD – The Transmit port of UART, by which embedded modules send data to the client (DTE)

USB (Universal Serial Bus) Interface

The USB interface in embedded modules is mainly for data transfer, it can also be used for communication and debugging. Typically, USB interface is a mandatory requirement for Type C/D modules and optional for Type A/B modules. Embedded modules should support a minimum of USB Full Speed (12 Mbps). The USB High Speed (480 Mbps) and OTG (On-The-Go) functions are optional.

UICC (Universal Integrated Circuit Card) Interface

Every embedded module must have a standard (ISO (International Standards Organisation) 7816-3 [9] based) UICC interface; it can also have embedded USB Inter-Chip (IC USB, defined in ETSI (European Telecommunications Standards Institute) TS 102 600) as an option. Embedded modules that support IC USB may reserve the IC USB package, once the IC USB is in use, the standard UICC interface is disabled. For Type C/D modules, the USB-UICC standard may be considered.

Antenna Interface

Every embedded module must have an antenna interface. Module must have an antenna pad or an antenna connector, for the antenna to be directly soldered to the module or connected to the module by a radio frequency cable.

GPS (Global Positioning System) Interface

A GPS antenna may be implemented in at least one of several ways:

- Shared with Primary WWAN, (Wireless Wide Area Network) antenna,

- Shared with the Diversity WWAN antenna,
- Separate antenna

An optional GPS antenna pad or antenna connector (that should be separated from the cellular antenna connector / pad) may be provided for the antenna to be directly soldered to the embedded module or connected to the embedded module by an RF (Radio Frequency) cable. Two types of GPS antennas to be considered are Passive and Active antennas. Active antenna (with internal low noise amplifier) requires voltage supply from the module via the antenna connector / pad.

SPI (Serial Peripheral Interface) Interface

The SPI interface in embedded modules is needed primarily for connecting external display equipment. The SPI interface may support master mode and/or slave mode. The module may have at least one SPI interface. It may support 4 ports as listed below or 3 ports for unidirectional transmission:

1. SDO – master data output, slave data input
2. SDI – master data input, slave data output
3. SCLK – clock signal, generated by the master
4. CS – slave enable signal, controlled by the master

I2C (Inter-Integrated Circuit Bus) Interface

The I2C interface in embedded modules is needed mainly for connecting external display equipment, or storage equipment. Typically, I2C is a mandatory interface for Type B/C/D modules and optional for Type A module. The transfer rate of the I2C bus must be at least 100Kbps; it can also be 400Kbps in the fast mode. The module with I2C interface is used as master controller.

1. SDA – serial data line
2. SCL – serial clock line

PWM (Pulse Width Modulation) Interface

The PWM interface in embedded modules is needed mainly for controlling indicating light, buzzer, analogue power output, and so on. For the type A/B/C modules, the PWM interface is optional. The type D module must have at least one PWM interface.

GPIO (General-Purpose Input / Output port) Interface

The GPIO interface in embedded modules is needed mainly for controlling external equipment, receiving external input signal. The number of GPIOs needed depends on the embedded application architecture.

ADC (Analogue-to-Digital Converter) Interface

The ADC interface in embedded modules is mainly for sampling external voltage/temperature data, and so on. For the type A/C modules, the ADC interface is optional. The type B/D modules must have at least one ADC interface.

SDIO (Secure Digital Input / Output) Interface

The SDIO interface in embedded modules is mainly for external SD card (Secure Digital card), or used as data transfer interface. For the SDIO interface is optional for type A/B/C modules, interface and mandatory for Type D modules.

AAI (Analogue Audio Interface)

The Analogue Audio interface in embedded modules is used for voice phone or voice transfer:

- The analogue input interface can be used for microphone or line-in,
- The analogue output interface can be used for line-out and direct driver receiver.

Embedded modules that support voice services may have at least one analogue audio interface, including one audio input interface and one audio output interface.

PCM (Pulse Code Modulation) Interface

The PCM interface in embedded modules is used for digital audio transfer. The module may also have a PCM interface. It is important for customers that the PCM clock should be a multiple of 128 KHz, for example, 256 KHz, 512 KHz.

Other interfaces

Embedded modules may also have other interfaces, for example, Keyboard/Power Key/Reset interfaces. All of these are optional, depending on the type of vertical application.

4.1.4.3 Guideline

The choice of hardware interfaces in each EM module will be decided by the manufacturers, depending on the type of vertical application. Required interfaces for all types of modules include power, UART/USB (communication interfaces), antenna and UICC. All other interfaces are determined by vertical use cases and considered in detail in vertical specific sub-sections in section 12.

4.1.5 Power Consumption

4.1.5.1 High Level Requirement

The power consumption of the embedded modules should be as low as possible and considered as part of the overall power budget of the host device.

4.1.5.2 Considerations

The power consumed by an EM device is dispersed across a number of features which may be implemented on the module. The PCI Express Mini Card has already specified the power requirements for 3G modules acting strictly as a data modem. The PCI Express Mini Card power requirements consider the peak current requirements for 2G and 2.5G devices in addition to as well as the normal current requirements for 3G devices. Additional power may be consumed by other features which are on-board.

The total power consumption requirements are determined by features included on-board of the embedded module and off-board features powered by the module.

Voltage input (V)	Feature	Operational Current Draw (mA)	Standby Current Draw (mA)
3.3 V	Data modem + UICC + GPS/A-GPS	2750 mA (peak) 1100 mA (normal)	250 mA (normal) (wake enabled) 5mA (normal) (not wake enabled) 2750 mA (peak) (wake enabled)

Table 7: Power Consumption Requirement by Module Feature

Additional power may be consumed by other features which are on-board the EM module such as:

- Application processing
- Communications (Bluetooth, WLAN, Zigbee and so on.)
- Sensors (accelerometer, humidity, temperature and so on.)
- I/O (SPI, I2C, PWM, ADC, SDIO, analogue audio and so on.)
- Camera

The host device may be able to perform power management by placing the embedded module into a low power state when the radio link is not being used.

4.1.5.3 Guideline

The EM module manufacturer shall publish the power consumption requirements considering features that are on-board the module such as the modem, communications, I/O and sensors.

The host device shall be designed with a sufficient power budget to host the EM module.

The host device should perform power management to minimize the power drained by the EM module.

4.1.6 Thermal Constraints

4.1.6.1 High Level Requirement

The embedded module should be sensitive to thermal constraints of a host device, and vice-versa.

4.1.6.2 Considerations

M2M applications generally involve thermal conditions that exceed the defined 3GPP temperature constraints. Three temperature ranges are herein identified for embedded applications, based on the average ranges of modules currently available in the market and requirements of different vertical use cases:

- Commercial -20°C to +55°C
- Industrial -30°C to +70°C

- Automotive -40°C to +85°C

3GPP does not define behaviour outside of the commercial temperature range other than “not to make inefficient use of the spectrum”. The performance effects of temperature should be made clear in the technical specification of the module.

4.1.6.3 Guideline

A host device must be able to calculate the heat generated by this device and provide a cooling mechanism. For example, power output can be reduced based on temperature monitoring.

To avoid overheating, the radio power should ideally be reduced to the minimum level of radio power needed to retain connectivity. Note however that power level is not fixed, but depends on factors such as distance to the base station. Radio power of the client in 3GPP networks is controlled by the network (that sends messages to the client for this purpose) and is therefore part of the network management.

Additional thermal guidelines that are applicable are described in the PCI Express Mini Card Electromechanical Specification in the section titled “Thermal Guidelines for PCI Express Mini Card Add-in Card Designers.”

4.1.7 IMEI (International Mobile Equipment Identity) / Device Identification

4.1.7.1 High Level Requirement

The Module integrated into the device must be uniquely identifiable.

4.1.7.2 Considerations

Please refer to “GSMA IMEI Allocation and Approval Guidelines” [1] for a discussion on IMEI considerations.

4.1.7.3 Guideline

In order for proper integration with service provider networks, each embedded device should be identified by means of an IMEI which uniquely identifies the hardware that contains the embedded functionality (embedded module). The IMEISV uniquely identifies the hardware in combination with its firmware version although this is not implemented consistently. Refer to “GSMA IMEI Allocation and Approval Guidelines” [1] for more details.

*4.1.7.4 **Security Guideline***

The embedded module shall implement a unique IMEI and protect it against tampering. For details, please refer to 3GPP document TS 22.016 [40].

4.1.8 Remote Diagnostics through Mobile/Wireless Network(s)

4.1.8.1 High Level Requirement

Some capability to monitor the status of an embedded module, and perform some level of diagnostic tests at a distance, and possibly whilst the module is in a moving vehicle is an extremely useful facility. Quite often in such cases it is difficult, costly or impossible to send a technician to the location of the module to carry out diagnostic work.

4.1.8.2 Considerations

Remote diagnostics demand a reliable communications link between the remote embedded module and the service provider’s diagnostic equipment. Solution designers need to design their applications with reference to the following factors which could affect the ability to complete diagnostic testing:

- The position of the module may affect its capability to transmit diagnostic information
- The reliability of its power source may make it necessary to provide some form of short-term backup power, to allow the module sufficient time to report a power loss alarm through the communications link in case of loss of main power source.
- If there is a necessity to minimise uplink traffic then compression of diagnostic logs may be needed (for example, HTTP compression/Gzip).
- In cases of uneven network coverage, it may be necessary to retry at intervals to establish a TCP/IP link until the module moves to an area of good network coverage.
- Some level of security to prevent unauthorised access to modules will be necessary. If password security is used, then there must be some method of password recovery to prevent a module becoming inaccessible
- Information contained in messages exchanged for remote diagnostics should generally be considered as sensitive, and consequently should be appropriately protected for security (for example, authenticity, confidentiality, integrity, repudiation, and freshness). TLS/SSL over TCP/IP should be used when transmitting sensitive data.

For simple regular status checks on a module, UDP (User Datagram Protocol) could be used instead of TCP/IP. In situations where data is very small (easily fits within one packet and is not at risk of fragmentation) and where packet loss and arrival order are not important, UDP minimises network traffic (and packet data costs) as it is a lower overhead protocol without the reliability, ordering, and congestion control of TCP.

Support of the following diagnostic features is considered essential:

- Initiate packet data protocol (PDP) context activation via SMS command
- Respond to “ping” query via ICMP
- Report module/device/subscription ids
- Report current serving cell ID, received signal level/ Received Signal Code Power (RSCP), scrambling code, location area ID and so on.
- Report current neighbour cells info; received signal level, ids
- Report stored history of radio link quality data
- Report circuit-switched call log (mobile-originated and mobile-terminated)
- Module stores key events in non-volatile memory then allows the log of these events to be uploaded via TCP/IP
- Start and stop log storage via remote commands
- Attach status (including reason for attach fail, if applicable)
- PDP context status (including reason for context establishment fail)
- Report hardware/software/firmware versions

The following diagnostic features may be optionally supported by a module:

- Report status of device integrity check of the HW/SW/configuration files of the embedded module
- Report status of device integrity check of the HW/SW/configuration files of the host device

- Report battery charge level
- Report packet transfer history statistics (number of Tx, number of Rx, retries)
- Report last 5 IP addresses with which the module communicated
- If module has location capability, report location
- If module or host device has a real-time clock capability, report local time
- Upload selected area of module memory (supplied address, length)
- Download and run an application in the module's RAM
- Check status of peripheral devices attached to module
- Report re-boot history (stored in non-volatile memory)
- Report stored history of local servicing of the module or the host device by technicians (including their ids)
- Re-boot module on remote command

Depending upon sensors connected to a module, it may also be possible to monitor environmental parameters such as:

- Temperature
- Pressure
- Humidity

OMA Device Management (DM) Diagnostics and Monitoring (DiagMon) [19] supports most of the diagnostic data mentioned above.

4.1.8.3 Guideline

A diagnostics application may run on the EM module or host device and make use of APIs or a serial diagnostic interface to extract diagnostic information and communicate it remotely.

The remote diagnostics should be carried out using a TCP/IP link to the module. A PDP context and hence a TCP/IP link may be initiated by sending a special MT SMS to the module.

Any such remote diagnostic functionality should be standardized, for example, in OMA DiagMon [19].

4.1.9 Local Mode System Diagnostics

4.1.9.1 High level requirement

If there is a problem which is preventing the embedded module from communicating with the cellular network, remote diagnostics will not be possible, and it will be necessary to send a service technician to test and repair/ replace the offending module. In this case some form of local diagnostic capability should be available to the technician.

4.1.9.2 Considerations

Some method of connecting diagnostic monitoring equipment will be necessary to allow service personnel to display information on the system status and diagnose any problems.

4.1.9.3 Guideline

A serial port should be provided on the embedded module which allows connection of the monitoring equipment (typically a PC with vendor specific diagnostic software). This port may or may not be available externally on the host equipment in which the module is embedded. Standard serial interfaces such as RS-232 or USB could optionally be provided on the host equipment for diagnostic access, or a special adapter could be used to provide the appropriate connection to the module.

The diagnostic interface should allow:

- Manual reboot
- Check of integrity of the h/w, s/w configuration of the module and/ or the host device
- Display of the cellular environment (for example, received signal strength, cell ids for serving and neighbour cells)
- List of any stored error codes or logs
- Display of selected log
- Display of non-volatile configuration settings
- Capability to test peripherals connected to the module
- Sending of at and diagnostic commands to the module
- Check of battery charge status

4.1.10 Supported Services

4.1.10.1 High level requirement

A basic set of services needs to be supported by all modules, with optional services for higher-end modules or modules targeted at specific vertical applications. The opportunity to employ these services will be governed by prevailing restriction of bandwidth, processing capability and/or memory capacity. In the following section, the following services are considered and guidance is provided on their use in embedded applications.

Basic set of services includes the following:

- SMS
- Packet switched data
- IP (IPv4/IPv6)
- TCP
- UDP
- ICMP

Optional services are typically available on higher-end modules or modules targeted at specific to particular vertical market, and include the following:

- Emergency Call
- MMS
- E-mail
- Circuit switched voice
- Circuit switched data

- Group 3 Fax
- Video call (3G only)
- Streaming video (3G only)
- Location Based Services
- MultiCall

Some of the above optional services may be necessary in specific use cases.

The details of each above-listed service and their application guidelines are listed below:

4.1.10.2 SMS

High Level Requirement

The Short Message Service is supported by all 2G and 3G networks around the world. Basic SMS allows up to 140 byte messages to be sent and received.

Considerations

SMS is by its nature a store-and-forward service, so there is no guarantee that there will be no delivery delay. SMS should not be used as the main method of communication in applications requiring guaranteed delivery or immediate (real-time) delivery.

Guideline

MO and MT (Mobile Originated and Mobile Terminated) SMS must be supported by all embedded modules as a basic means of communication with the cellular network. It can be used as a fall-back low bit rate communications channel if a higher rate circuit or packet switched data channel is not available.

4.1.10.3 Packet Switched Data

High Level Requirement

Packet-switched data services are essential to support TCP/IP internet connectivity.

Considerations

All 3GPP networks around the world support a variant of packet data service. Examples are GPRS, EGPRS (Enhanced General Packet Radio Service), High Speed Packet Access (HSPA) and LTE (Long Term Evolution).

Guideline

At least one of these services is mandatory for all classes of embedded module. The higher data rate services are necessary for more data-intensive applications that might require higher throughput, lower latency and/or improved quality of service (QoS).

4.1.10.4 IP

High Level Requirement

IP is the basis for most packet-based services, supporting TCP and UDP as well as lower-level services such as ICMP. All embedded modules need IP.

Considerations

IPv4 is likely to be required for most embedded devices, but in some cases an IPv6-only module may be preferable (for example, a device that does not need to access currently deployed services over IPv4, such as a smart meter or dedicated device). IPv6 is becoming more widely used, and, because it eliminates the resource constraint on the number of IP addresses, is very attractive for embedded modules. With IPv6, operators need not be concerned with the number of IP addresses used by modules.

Guideline

IP is an essential, mandatory service for all types of embedded module.

4.1.10.5 TCP

High Level Requirement

All embedded modules need Internet connectivity via TCP. This is the basis of communication for most EM applications.

Considerations

The embedded module must provide at least one packet-switched data service to support TCP.

Guideline

TCP is an essential, mandatory service for all types of embedded modules.

4.1.10.6 UDP (User Datagram Protocol)

High Level Requirement

Depending on the particular situation, UDP may have a lower protocol overhead than TCP. UDP tends to be favoured in applications which demand many small data transfers; for example, polling the embedded module on a regular basis to check status. This is especially true when the data to be transmitted easily fits within one packet and is not at risk of packet fragmentation, and where packet loss and packet arrival order are not a concern.

Considerations

UDP uses the same packet-switched data services as TCP, and has no impact on module cost.

Guideline

This service should be available as an optional alternative to TCP on all classes of embedded module.

4.1.10.7 ICMP (Internet Control Message Protocol)

High Level Requirement

ICMP is a fundamental aspect of the IP protocol suite, and is generally supported by the IP stack. It is not used by applications directly, but rather provides low-level support to IP services, including ping (test for device reachability or reachability by the device to other services) and notification of traffic/connectivity status (host or network reachability status and reason, and so on.).

Considerations

ICMP uses the same packet-switched data services as TCP, and has no impact on module cost. When IPv6 is supported, ICMP6 should also be used.

Guideline

ICMP should be available for diagnostic and other purposes on all classes of embedded module.

4.1.10.8 Emergency Call

High Level Requirement

Emergency call is an automotive-specific service. eCall is a European Commission specified (in Europe) emergency service for the automotive vertical sector.

Considerations

3GPP has specified that the Minimum Set of Data (MSD) for an incident is transferred to the Public Safety Answering Point (PSAP) via an in-band modem method (see 3GPP TS 26.267 [41]) using the same speech channel as the voice call. This means that the specific algorithms in 3GPP TS 26.267 must be used to implement eCall capability. This may prove to be difficult or impossible to implement on some existing embedded modules, as it would be necessary to break into the speech path, and integrate the additional (de)coding, (de)multiplexing and (de)modulating functionality onto the Digital Signal Processor (DSP) of the embedded module's chipset. There may be limitations on the processing and memory capacity of a module which prevent these design modifications.

Guideline

Emergency Call should be supported by any modules supplied for emergency purposes to the automotive vertical sector.

A module supporting both GSM and UMTS radio technologies (dual-mode) should facilitate greater flexibility in responding to different cellular network evolution paths across Europe for a longer period of time (i.e. more likely to correspond to the lifetime of the vehicle).

4.1.10.9 MMS (Multimedia Messaging)

High Level Requirement

MO MMS is used typically in embedded modules for capturing still photographs or video clips sent for security monitoring purposes or in consumer embedded devices.

Considerations

MMS relies upon Wireless Application Protocol (WAP) as a transport mechanism.

Standard Internet e-mail is an alternative to the MMS service. A still picture, video or audio clip may be sent using the ubiquitous Multi-purpose Internet Mail Extensions (MIME) format, with many forms of encoded attachment.

Guideline

This service is optional for all classes of embedded module.

4.1.10.10 E-mail

High Level Requirement

There may be a requirement in some EM applications to automatically generate outgoing (mobile originated) e-mail messages with attachments (for example, a security/ surveillance application). Also in consumer applications, it may be necessary to support the sending and receiving of e-mails. In some cases, email may be used to provide an automated store-and-forward mechanism for transmitting data to an application (for example, in the way that printers can use email to receive documents for printing). The store-and-forward nature of email allows a device that is out of coverage to receive messages when it has coverage; this can be an alternative to a lower-level mechanism such as a custom server holding data until a device can receive it.

Refer to: "Internet Mail Architecture" (RFC 5598) for further information.

Considerations

An e-mail client which supports the standard Internet protocols must be provided to support this service.

When transmitting outgoing (mobile originated) messages, the device should use the "Message Submission for Mail" protocol as specified in RFC 4409. Message Submission is the preferred and standard way for email clients to submit messages.

To support incoming (mobile terminated) e-mails, either POP3 (Post Office Protocol, RFCs 1939, 2449 and 5034 and so on) or IMAP (Internet Message Access Protocol – RFC5593 and so on.) protocols must be supported, and a mailbox must be available on a server accessible by the device (for example, using TCP over the Internet). When using IMAP, a number of extensions are available to improve performance or meet certain needs. The so-called "Lemonade" profile for mobile email (RFC 5550) is specifically designed for make it easy for "clients (especially those that are constrained in memory, bandwidth, processing power, or other areas) to efficiently use IMAP and Submission to access and submit mail."

The Submit protocol (RFC 4409) can be implemented in the case of email transmitting only devices.

A still picture, video or audio clip may be sent as an attachment via e-mail by using Multi-purpose Internet Mail Extensions (MIME) (Ref: IETF RFC2045).

Data specific to an application may be sent to the device as a custom (vendor-specific) MIME format. Anyone can register a vendor-specific MIME content type (for example, "application/vnd.company.application"). See http://www.iana.org/assignments/media-types/application/ for current values.

If security (integrity protection or privacy) of account credentials, messages or attachments is important, the use of transport layer (hop-by-hop) or application layer (end-to-end) security extensions may be necessary. Transport Layer Security (TLS, RFC 4346) is very commonly used to protect data hop-by-hop. Simple Authentication and Security Layer (SASL) (RFC5034, RFC 4959 is widely used to protect account credentials. Either Secure/Multipurpose Internet Mail Extensions (S/MIME, RFC 5751) or Pretty Good Privacy (PGP, RFC 2015) can be used to protect email messages end-to-end. TLS can also provide compression for email messages, which reduces bandwidth requirements and can save battery life and power consumption (by reducing the amount of time the radio is active). See Transport Layer Security Protocol Compression Methods, RFC 3749, and the Lemonade Profile (RFC 5550) for more information.

Guideline

This is an optional service for all embedded module types. If e-mail capability is required, the necessary Internet protocols must be implemented either in the embedded module or on the host device.

4.1.10.11 Circuit Switched Voice

High Level Requirement

This service provides a one-way or two-way speech call to be set up between the embedded module and the cellular network or fixed telephone network.

Considerations

Most M2M applications do not require speech calls. However, some security applications provide the option for an emergency call (MO/MT - Mobile Originated/Mobile Terminated). In Europe eCall is a mandatory requirement for the automotive vertical sector, and requires circuit switched voice call support (see details below).

Guideline

In applications where speech is required the module should, as a minimum, provide support for all the narrow band codecs: GSM (half rate, full rate, enhanced full rate) and adaptive multi-rate narrowband (AMR-NB).

For eCall in Europe, circuit-switched voice must be supported together with in-band modem capability. If circuit-switched data support is provided, both transparent and non-transparent asynchronous services up to at least 9600 bits/s should be supported.

4.1.10.12 Circuit-Switched Data

High Level Requirement

The various low bit rate circuit-switched bearer data services (from 300 to 14,400 bits/sec) may be required by some legacy applications. Usually only asynchronous circuit-switched data services are supported. Circuit-switched data services may be used as a fall-back if packet-switched data services are not available.

Considerations

Many network operators around the world have started to drop support for circuit- switched data services, so these services can no longer be relied upon for use globally. Some countries however have limited packet-switched data services support and therefore will require circuit-switched support.

Guideline

Circuit switched data should be treated as an optional service that is used in some countries/ regions to support legacy applications or due to lack of packet-switched network coverage, for example, in areas that do not have any GPRS coverage.

4.1.10.13 Group 3 Fax

High Level Requirement

Group 3 Fax Teleservice provides the capability to send and receive faxes from the embedded module.

Considerations

The Fax Teleservice requires a 9600 bits/sec transparent circuit switched data bearer. If this bearer is not available on a network, it will not be possible to support Group 3 Fax (refer to Circuit Switched Data service above).

This is an uncommon service, and its benefits for most EM applications are not obvious. One application of Group 3 Fax in an embedded module would be in a fixed/ wireless desktop device, but this would not allow a standard fax machine to be connected as this uses an analogue 2 wire-interface.

Group 3 Fax is usually only used for MO (Mobile Originated) faxes generated by a fax software application. MT (Mobile Terminated) faxes are more difficult to achieve, as they require the module to have an additional special telephone number MSISDN, (Mobile Station International Subscriber Directory Number) dedicated to the fax service to receive the MT fax data call. This would require a specially configured SIM/USIM and an additional network subscription.

Guideline

This service is optional and vertical-dependent.

4.1.10.14 MultiCall

High Level Requirement

Multi call improves usability by enabling simultaneous multiple connections such as Voice and Data.

Considerations

For 2G/2.5G modules, support of Dual Transfer Mode (DTM) or GPRS Class A operation would be necessary to provide even limited multicall capability (maximum of 1 speech bearer and 1 data bearer simultaneously).

Guideline

The service requirements are provided in 3GPP TS 22.135 [43].

This service is optional and only feasible on 2.5G or 3G modules with higher processing power and memory capacity, and thus relevant for specific vertical applications, such as automotive.

For the automotive vertical, this service could be used to provide a similar functionality to eCall whereby data containing information on the status and position of a vehicle involved in an accident could be transmitted whilst an automatically initiated voice call to the emergency services was in progress.

4.1.10.15 Video Call

High Level Requirement

There may be requirements whereby a video call supplements other communication modes for emergency or security considerations in EM applications.

Considerations

Bi-directional real-time video is not a common requirement for M2M applications. If real-time video capability is required on an embedded module, it is usually only on the uplink for monitoring purposes. Therefore it is more important to have a high bandwidth available on the uplink than the downlink for example HSUPA (High Speed Uplink Packet Access) would be required rather than HSDPA (High Speed Downlink Packet Access).

Guideline

This is an optional service which is only required for specialist applications on 2.5G and 3G embedded modules with higher processing power and memory capacity to cope with the video processing and buffering.

4.1.10.16 Streaming Video

High Level Requirement

High-end security systems may require to stream video captured from a surveillance camera to a service centre operator, for example.

Considerations

The packet-switched streaming service (PSS) provides an adaptive streaming capability which is suited to video. Various video codecs need to be supported for streaming: H.263, MPEG-4, and H.264 (AVC).

For surveillance applications it would be necessary to implement a PSS server (RTP or HTTP based) in the embedded module. This is the exact opposite of the more common usage of video streaming; that is, to allow a user to watch films or clips on their handset that are stored on a central server.

Data rates as low as 128kbits/sec may be used across the air interface, so it should be possible to support video streaming on 2.5G and 3G networks from EGPRS upwards.

Guideline

This is an optional service which is only required for specialist applications which would feature in embedded modules with broadband capabilities (2.5G and higher), high processing power and memory capacity to cope with the video processing and buffering.

4.1.10.17 Location Based Services

High Level Requirement

Knowledge of the geographical position of an embedded module is necessary in many applications. The position information may be used to provide various location based services.

Examples of location based services are:

- Emergency services
- Personal tracking
- Geo-fencing
- Asset tracking
- Vehicle fleet management
- Local area information

Considerations

Various methods or a combination of methods may be used to determine the embedded module’s location:

- Cell ID/ received signal strength
- Base station time differences
- GPS
- Assisted GPS (A-GPS)

Refer to 3GPP TS 23.271 [44], TS 25.305 [45], and OMA SUPL [20]for further information.

The required accuracy and reliability of position depend upon the application. The most critical applications are those such as emergency services and vulnerable person tracking.

There may be privacy issues associated with tracking an individual's position. It may be necessary to allow a user to disable the location tracking capability.

GPS hardware may consume large amounts of power, which may reduce battery life on portable systems. A suitable power management strategy should be implemented to mitigate this issue.

Guideline

The location based services are optional in many applications, but mandatory for some applications to support other services, for example, eCall.

If location information is required, the most appropriate location method should be implemented on the embedded module according to the particular application.

The most reliable and accurate location information is obtained by using A-GPS (Assisted GPS) which combines location information from cell locations, a network database and GPS satellite data to provide a fix of the embedded module’s position. The assistance capability also minimises the Time To First Fix (TTFF) from GPS start-up which may be important in some applications.

4.2 Guidelines Regarding the Radio Interface

4.2.1 Radio Technologies Supported

4.2.1.1 High level requirement

EM Device users require connectivity ranging from fixed low data rate applications to mobile broadband anytime and anywhere.

4.2.1.2 Considerations

The range of embedded modules is designed to provide the end-user with cellular connectivity with specific module types providing integral connection management for 2G, 3G and beyond.

4.2.1.3 Guideline

The embedded module shall support at least GPRS for the low date rate module type and WCDMA/LTE (optional) for the high data rate offering. In future additional radio technologies may be considered. Radio Coexistence and Frequency Bands

4.2.1.4 High Level Requirement

Attention to coexistence with other wireless technologies likely to be resident in the same unit is required. There should **never** be any interference between the 3GPP radio interface and other radio interfaces present in the embedded device.

4.2.1.5 Considerations

Wireless technologies that could be integrated into an embedded device may include:

- DVB-H
- DVB-T
- FM radio
- GSM
- GPRS
- EDGE
- WCDMA
- LTE
- cdma2000 1xRTT
- cdma2000 1x EV-DO
- HSPA
- GPS
- Bluetooth
- WLAN 802.11a/b/g/n
- UWB
- Zigbee

4.2.1.6 Guideline

The EM radio should always adhere to the local regulatory rules on co-located transmitters and receivers.

Proper isolation based on spatial separation and front-end filtering should be considered to meet the interference requirements of each individual wireless technology. Specifications of antenna isolation between wireless technologies should be developed to minimise interference and to maximise throughput performance.

4.2.2 Radio Interference with Device Components

4.2.2.1 High Level Requirement

The EM functionality must be integrated with the host device (for example, car, medical device and so on.) in such a way as to minimise any possible interference with other components.

4.2.2.2 Considerations

Embedded host devices may have complex electromagnetic environments with a multitude of highly integrated components and circuit types. Interference in a host embedded device is typically sourced from circuits such as CPU, memory chips, video circuits and other components generating high frequency noise which has the potential to couple into the embedded cellular radio through the antenna or other conducted paths. Such interference affects the overall wireless performance and User experience.

4.2.2.3 Guideline

The embedded device design must consider the integration of a cellular radio and minimise interference between the host system components and the embedded module and associated antenna subsystem.

4.2.3 Radio Power

4.2.3.1 High Level Requirement

The radio power should be set to such levels that comply with the network requirements and the integrated product should be designed to comply with regulatory safety requirements.

4.2.3.2 Guideline

The integrated product design should take into account individual radio transmission characteristics in addition to as well as simultaneous transmissions from all radios in order to comply with Specific Absorption Rate (SAR) limits.

4.2.4 Antenna Location and Characteristics

4.2.4.1 High Level Requirement

The antenna should be configured and placed to optimise radio performance within the constraints of the (physical) host device design.

4.2.4.2 Considerations

Antennas play a critical role in the performance of the wireless communications and are considered a key element in the design and implementation of embedded modules. The location in the host device, exposure to interference, size and type of cabling are critical in the overall performance of the modem measured in terms of throughput rates, number of dropped connections and thus User experience and satisfaction.

4.2.4.3 Guideline

Since the antenna is a key component for enabling wireless technology, its critical design parameters such as mounting location and space allocation should be considered in the early phases of the host device development process in order to maximise its performance. Grounding and metal clearance near the antenna feed point are strongly recommended to provide consistent radiated performance in production. Pattern shape is another antenna performance parameter that should not be overlooked. An omni-directional type pattern is more desirable than the directional one. Parasitic coupling to metal structures near the antenna can alter its pattern shape and operational bandwidth.

To minimise interference, it is preferred that the position of the antenna is as far as possible from any digital circuitry that generates high frequency noise (that is, high speed clocks). In addition, techniques such as antenna diversity can be considered to improve system throughput performance and reduce interference.

The antenna gain of the host device should comply with 3GPP TR25.914 [46].

4.2.5 Antenna Performance for Mobile Receive Diversity (MRD) for 3G connectivity

4.2.5.1 High Level Requirement

Mobile Receive Diversity (MRD) is a feature if properly implemented can significantly enhance Forward Link (FL) capacity of the network and 3G throughput performance of the host device. It is highly recommended this function to be implemented in 3G capable embedded host devices. A MRD-capable modem and a secondary receive-only antenna are required for this 3G performance-enhancement feature. For host devices with embedded 3G modem, the secondary antenna should be integrated inside the host to provide optimum and consistent performance.

4.2.5.2 Considerations

MRD is intended as a feature that only enhances and does not degrade network performance. At a minimum, the primary antenna of an MRD-capable device should have the same electrical performance as that of a single-antenna non-MRD device since the existing networks were deployed based on the pre-established performance of the non-MRD devices. Furthermore, the transmit function of a MRD-capable device relies solely on the primary antenna. Since the secondary antenna is used only for the receive function, its required bandwidth is less than 50% of the full bandwidth of the primary antenna. This allows for a smaller antenna to be used as the secondary antenna. Similar to the considerations given to the primary antenna, the mounting location of the secondary antenna in the host device, its exposure to interference and type of cabling used should be considered in the integration process of the secondary antenna in order to achieve diversity gain. The addition of the secondary antenna should not impact performance of the primary antenna.

4.2.5.3 Guideline

The effectiveness of MRD depends on the key antenna performance parameters such as antenna efficiency, pattern correlation and isolation between antennas. The recommended antenna performance goals are provided in the following table:

Type of Antenna	Antenna Performance Criteria	Performance Goals
Main Antenna (TX and RX)	Primary Antenna Efficiency (including cable loss)	> -4 dB
	V-pol Gain / H-pol Gain	> 0 dB
	VSWR in Free Space	< 3:1
Diversity Antenna (RX)	Efficiency of Diversity Antenna Including cable loss	> -7dB *
	Main to Diversity Antenna Isolation	> 10dB
	VSWR in Free Space	< 3:1
	Envelope Correlation Coefficient (ρ_e)	**(ρe) =** < 0.5

* Note: The secondary diversity antenna can be up to 3dB worse in gain than the primary antenna and still provides diversity

Table 8: Recommended Antenna Performance Goals for 3G MRD-capable Host Devices

4.2.6 Recommended Minimum Radiated Performance Requirements – 3G

4.2.6.1 High Level Requirement

The embedded module and embedded host device shall meet minimum radiated performance requirements to prevent a direct impact to overall mobile network efficiency and ensure a good end user experience in terms of performance that is, data rates and coverage.

The following recommendation is for 3G network compatibility only. It should be noted that devices will also be required to comply with requirements for 2G networks to allow for connectivity in areas where there is no 3G.

Embedded host device manufacturers should discuss 2G TIS (Total Isotropic Sensitivity /TRP (Total Radiated Power) requirements directly with their service provider partners.

4.2.6.2 Guideline

Radio performance of mobile devices is expressed in terms of free-space TIS [dBm]) and TRP ([dBm]) parameters. TIS and TRP are the relevant parameters when considering radiated performance of host devices that have a form factor that allows for the use of the standardized TIS and TRP test procedures.

For those host devices for which standard TIS/TRP procedures can be applied the minimum values recommended for the 3G host device, as described in section 4.2.6.3and 4.2.6.4

The following points should be noted when designing product in accordance with the recommendations:

- The TIS/TRP values are relevant only for data services (even if a 12.2 kbps reference channel is employed for W-CDMA measurements).
- The minimum values shown in this document will be considered when presenting a device for service provider certification. However additional or more stringent requirements may apply according to service provider network and service configuration.
- TIS/TRP tests should be performed in accordance with the CTIA procedure “CTIA Test Plan for Mobile Station over the Air Performance, Revision 3.1 ".

4.2.6.3 TRP Recommendation

TRP Limits

Technology	Average TRP (dBm)
3G UMTS Power Class 2[‡]	**20[‡]**
3G UMTS Power Class 3	**17**
3G UMTS Power Class 4	**14**

"Average TRP" represents the linear average of the TRP values measured at the low, mid, and high frequencies at each band, adapted from the definition in 3GPP 25.144, Section 6.1:

$$TRP_{average} = 10\log\left[\frac{10^{TRP_{low}/10} + 10^{TRP_{mid}/10} + 10^{TRP_{high}/10}}{3}\right]$$

where TRP_{low}, TRP_{mid}, and TRP_{high} are the single-channel measurements, expressed in dBm.

[‡] 3GPP conducted transmit power specification for Power Class 2 only defined for Operating Band I: 27dBm (+1/-3dB)
Consensus TRP limit of 20 dBm derived based on 3 dB delta between conducted specs for PC2 and PC3

4.2.6.4 TIS Recommendation

TIS values are defined with reference to a **single-antenna receiver**. TIS test should be performed in accordance with the CTIA procedure “CTIA Test Plan for Mobile Station over the Air Performance, Revision 3.1 ".

Technology	Average TIS (dBm)
3G WCDMA 850	-96
3G WCDMA 900	-99
3G WCDMA 1800	-101
3G WCDMA 1900	-101
3G WCDMA Band I	-101

WCDMA TIS defined with respect to BER=0.012 @ 12.2 kbps
EDGE TIS defined with respect to BLER=0.1 @ MCS-5

"Average TIS" represents the linear average of the TIS values measured at the low, mid, and high frequencies at each band, adapted from the defintion in 3GPP 25.144, Section 7.1:

$$TIS_{average} = 10\log\left[3\Big/\left(\frac{1}{10^{TIS_{low}/10}} + \frac{1}{10^{TIS_{mid}/10}} + \frac{1}{10^{TIS_{high}/10}}\right)\right]$$

where TIS_{low}, TIS_{mid}, and TIS_{high} are the single-channel measurements, expressed in dBm.

4.2.6.5 Radiated Performance at Intermediate Channels

For each band, radiated performance at the intermediate frequency channels (where TIS was not measured) shall be evaluated.

Radiated sensitivity at each intermediate channel shall be within 5 dB of that of the nearest frequency at which TIS was measured. This shall be verified using the relative method for intermediate channel sensitivity defined by CTIA [57] or a peak sensitivity scan at the same channels.

4.2.6.6 Radiated Performance for Large Form Factor Host Devices

4.2.6.7 High Level Requirement

For large form factor devices (for example, cars, automatic teller machines and so on) the standardized TIS and TRP test procedures cannot be applied. As the radiated performance of the host device with embedded antenna and embedded module is critical to in-service performance and network efficiency, it is important to make an assessment of the radiated performance at host level using other methodology

4.2.6.8 Considerations

Radio performance of large form factor host devices can still be evaluated in terms of free-space TIS [dBm] and TRP [dBm]) parameters with an assessment that considers the simplified definitions:

Definition of Total Isotropic Sensitivity can be simplified to:

$$TIS = \frac{P_s \cdot \Delta N_0}{\eta}$$

- Ps = Conducted sensitivity
- η = Antenna efficiency (including cable losses, and so on.)
- ΔNo = Noise floor elevation due to radiated self-jammers (AWGN)

4.2.6.9 Guideline

The conducted sensitivity and conducted tx power is evaluated and certified at the module level and if necessary can also be readily evaluated in-situ (connected to the host device). For large form factor host devices it is expected that antenna are off-module and integrated into the host. The antenna efficiency can be assessed through test or simulation. The noise contribution from the host device can be assessed using the noise signature methods referenced in section 7.

If the embedded module is tested and certified using a “reference antenna” and a comparable antenna is used in the host device then this may be sufficient to demonstrate compliance with operator radiated requirements and obtain certification for the host device.

4.2.7 GPS and A-GPS

4.2.7.1 High Level Requirement

The GPS radio receiver and antenna must operate with high sensitivity and needs a low noise environment on a multi-radio embedded host device.

4.2.7.2 Considerations

The presence of other wireless signals and electrical side effects should not significantly degrade GPS performance. The host device manufacturer must ensure coexistence and concurrence in their design integration of the environment considering antenna design, radio emissions and adjacent bands. GPS operation should not require the other wireless technologies to shut down. One reason for this requirement is that locations from GPS are often fed into an Internet application connecting at the same time over the cellular radio. The hardware and antenna solution for certification should be harmonized with other radios including:

- 802.11 a/b/g/n
- Bluetooth
- WWAN (for example, GSM/ /GPRS/EDGE/UMTS/HSPA/LTE)
- Broadcast
- FM Radios
- Other emerging wireless radios

4.2.7.3 Guideline

GPS should coexist with other wireless technology on the embedded host device.

4.2.8 Antenna Performance for GPS

4.2.8.1 High Level Requirement

Embedded modules can offer a Global Navigation Satellite System[2] (GNSS) such as GPS. GPS requires implementation of a receive antenna in the embedded device.

[2] Other GNSS systems, such as Galileo (Europe) and Beidou (China) are currently under development and additional antenna performance requirements might emerge in the near future. The outlined requirements are only applicable for GPS.

4.2.8.2 Considerations

GPS antenna options

To support the GPS feature implemented in the embedded module there are typically three options for implementing a GPS antenna in the embedded device:

1. Share with Primary Antenna

For GPS, the antenna is used to receive only. However, the primary antenna is also used by the embedded module to transmit signals to the cellular network. As a result, there must be good front end isolation on the embedded module between the GPS receive path and the 3GPP radio transmit path to avoid cross talk and degradation of the GPS signal. Additionally, a triplexor is needed to enable the primary antenna to simultaneously receive across several bands (ex. 850 MHz, 1900 MHz, 1500 MHz for GPS). The triplexor and a send/receive switch introduces insertion loss which degrades the GPS receive signal.

2. Share with Diversity Antenna

The GPS signal is received on the diversity antenna along with 3GPP radio signals which are used for the mobile receive diversity function. Again, a triplexor is needed to enable the GPS and 3GPP radio-receive signals to be processed simultaneously. The diversity antenna must be suitably isolated from the primary antenna to minimize leakage of the 3GPP radio transmit signal back into the GPS receive path. The implementation of receiving the GPS signal on the diversity antenna is beneficial compared to using the primary antenna: less insertion loss; less number of bands to cover, more spatial separation from 3GPP radio transmitting signals on the primary antenna.

3. Standalone antenna

A standalone GPS antenna requires the presence of an additional antenna in the device dedicated to GPS. Additional costs are incurred for the antenna, cable and the consumed space impact. The standalone antenna must be suitably isolated from all other transmitting antennas to minimize leakage of signal transmissions of other antennas back into the standalone antenna.

All three antenna options have been implemented in commercial mobile phone platforms. The chosen antenna option may be driven by module layout. The PCI Express Mini-card form factor, for example, provides two antenna leads on the card thereby enabling any of the above solutions.

Polarization

GPS signals employ Right Hand Circular Polarization (RHCP). Embedded modules employ linear polarization on the antennas for the radio signal. A linearly polarized antenna will pick up a RHCP signal (since it is spinning). However, the GPS signal will be degraded by 3dB because the linearly polarized antenna only receives about half of the power generated by the RHCP GPS signal. Once a GPS signal is received indoors, it may bounce and become reverse polarized. The linearly polarized antenna can still pick up such a signal.

Spatial Pattern Coverage

The spatial pattern coverage refers to the area around the device where the GPS antenna can pick up the GPS signal. The spatial pattern coverage impacts the number of satellites in a user's Field Of View (FOV). The pattern should be at least a half-sphere (preferably spherical) that goes around the device (to pick up the GPS signals from the sky). The considerations for spatial pattern coverage may be different for indoor or outdoor use. When designing the spatial pattern coverage, it is also important to account for shadowing and absorption effects of the embedded device enclosure and position of the user's body relative to the device.

Antenna Average Gain

The received signal level is a dependent on the strength of the electromagnetic waves from the satellites at the user's location and the device antenna gain in the direction of these waves.

The average antenna gain refers to spatial average of the antenna gain over the field of view. Antenna gain is calculated in this manner since signals can come from multiple satellites and from random, multiple directions due to scattering.

The value of average antenna gain has a direct correlation to the GPS receiver sensitivity. If the antenna gain is 1dB less, the signal to noise ratio must be 1dB greater to compensate, otherwise there will be a drop in number of GPS fixes.

Antenna to Antenna Isolation

The GPS antenna must coexist with other antennas which are simultaneously transmitting signals such as 3G, WLAN and WPAN. Energy received from other transmitting antennas can jam the GPS signal.

4.2.8.3 Guideline

The effectiveness of the GPS feature depends on the key antenna performance parameters such as selection of GPS antenna option, polarization, spatial pattern coverage, antenna average gain, and antenna-antenna isolation. The recommended antenna performance goals are provided as follows:

Parameter	Performance Goal
GPS antenna option	GPS signal received on diversity antenna
Polarization:	Linearly polarized antenna
Spatial pattern coverage:	Half-sphere (preferably spherical)
Antenna average gain:	> -4 dBi including cable loss
Antenna-Antenna isolation:	>10 dB

Table 9: Recommended Antenna Performance for GPS

4.3 Guidelines Regarding Mobile Broadband Traffic Offloading

As mobile data traffic has increased rapidly, there is emerging need for efficient use of existing networks due to the following reasons.

As mobile data traffic remains to increase explosively, it can burden the network considerably. Absorption of large amounts data traffic in the network can deteriorate voice call capacity due to the lack of network capacity for voice traffic. Hence additional capex is required to cover the increased data traffic. Costs of network operation and maintenance will also increase.

To alleviate the surge in network resources due to the data usage, alternative use of the available networks could be possible.

Offloading to Wi-Fi is most popular, but offloading to other network technologies also can be possible, for example Femtocells. Offloading can lead to efficient use of existing network resources, whereas:

- Dispersion in load factor in traffic will be maximized
- TCO is expected to decrease

- Call capacity is expected to improve in voice services
- CAPEX for additional data traffic will be mitigated
- Customer satisfaction will increase due to the improved service quality.

To provide secure connectivity (that is, provide the same secure environment as in cellular networks) the current network authentication mechanism could be implemented to ensure seamlessly offloading traffic over other networks.

4.3.1 UICC as Authentication Token for Different Applications and Other Radio Technologies

4.3.1.1 High Level Requirement

The user requires a simple and unambiguous way to connect to different kinds of networks without having to supply credentials for each network.

4.3.1.2 Considerations

Wireless service on devices can be implemented through a variety of radio technologies, including, but not limited to 3G and WLAN. In all cases, secure authentication between the User and the wireless service provider is critical.

The UICC, given its inherent physical and logical security features, its portability, and multi-application architecture (SIM, USIM, and EAP-UICC) can be used as a single authentication token for all radio technologies. The UICC applications (USIM or ISIM) also enable mutual authentication in the IP Multimedia Subsystem (IMS).

Access to EAP-SIM and EAP-AKA is required to start an authentication negotiation between the device client and a central authentication server. This can be used to establish (U)SIM authenticated sessions. Examples are a WLAN access session at a hotspot or entering an IKEv2 negotiation to establish an IPSEC session.

4.3.1.3 Guideline

If the UICC is used for authentication for Wi-Fi Access, it is recommended that Wi-Fi Certified WPA-2 with EAP-SIM / EAP-AKA is used.

In case an UICC is not used for Wi-Fi authentication, the use of Wi-Fi Alliance certified authentication methods is recommended.

4.4 Guidelines Regarding the UICC

4.4.1 Form Factor of the UICC Reader

4.4.1.1 High Level Requirement

In some vertical markets the use of the existing standard UICC form factor may not meet the size requirement in addition to environmental and operational considerations. As a result other form factors must be considered as determined by the needs of the vertical markets. A tamper-resistant hardware component is required to properly protect the network access credentials.

4.4.1.2 Considerations

Because of considerations such as the varying sizes of the devices in the different vertical markets, the potential need to limit accessibility, and potentially extreme environmental considerations, the current standardized UICC form factor may not be appropriate for some of the applications in some vertical markets. It becomes necessary therefore to identify other form factors that will meet the different vertical market needs not supportable by the current standard UICC.

In addition to the current standardised UICC known as “plug-in”, other form factors that may be considered include the 3FF (mini-UICC) defined in ETSI 102 221 [27] and the new M2M UICC defined in ETSI TS 102 671 [28].

The Plug In form factor or the mini-UICC form factor (a.k.a. 3FF) defined in ETSI TS 102 221 may be used in M2M environments provided that the UICC connector meets the environmental constraints of the target environment. For these form factors, hardened connectors that ensure proper electrical contacts under vibration and shock conditions may be needed in some vertical markets.

The ETSI TS 102 671 has developed an M2M specific UICC form factor of size 5mm x 6mm that supports automatic pick-and-place process for mounting on the module and could be used through a connector with reduced footprint to preserve removability. Use of this permanently affixed form factor may require a standard mechanism to choose a new operator to provide service to an embedded device.[3]

4.4.1.3 Guideline

The precise form factor of the UICC is to be decided by the embedded module vendors and embedded device manufacturers, for whatever module type, depending on device constraints, the vertical market and targeted use cases. Due consideration should however be given to the constraints and guidelines discussed throughout section 4.4.

4.4.2 Location of UICC Reader

4.4.2.1 High Level Requirement

When determining the location of the UICC reader, consideration must be given to the need for accessibility of the reader for placement and removal of the UICC as determined by each vertical market and use case requirements.

4.4.2.2 Considerations

In some vertical market use cases, ready accessibility (for example, by the end user/customer) may not be desirable.

In other use cases, where accessibility of the UICC for placement and removal may provide convenience, the UICC reader in an embedded device may or may not be integrated within the embedded module.

UICCs can either be installed during manufacturing (supplied by the service provider through an original equipment manufacturer (OEM) agreement) or inserted by the User. Please refer to section 4.4.2 for a discussion on the accessibility of the UICC.

4.4.2.3 Guideline

The precise location of the UICC or UICC Reader is to be decided by the embedded module vendors in conjunction with the embedded device manufacturers. It can be on the module or on a host device. Due consideration should however be given to the constraints and guidelines discussed throughout section 4.4, and specifically also to section 4.4.4 (Insertion/Removal).

[3] The considerations to accomplish this capability are currently being studied by the GSMA Embedded SIM project. Once the project output has been published the output will be available for review and subsequent updating of this section.

4.4.3 Physical Connection between UICC Reader and Embedded Module

4.4.3.1 High Level Requirement

The UICC needs to be physically and logically connected with the embedded module to allow flow of data and power.

4.4.3.2 Considerations

Due to the small size of some modules, physically accommodating a UICC reader on some embedded modules may not be practical.

4.4.3.3 Guideline

If the UICC Reader is not co-located on the embedded module, it should at least be ensured that the UICC Reader is uniquely associated with a single relevant embedded module and connected to it via hardwiring. The distance should not lead to the signal degradation. It is proposed that connection of the UICC Reader to the embedded module adheres to 3GPP TS 31.101 [7] which is the 3GPP standard defining the physical and logical characteristics of the UICC - terminal interface to which UICC hosting (U)SIM and / or ISIM shall comply.

4.4.3.4 Security Guideline

The UICC reader which is used for authentication by an embedded module shall be directly (electrically) connected to the embedded module, not using a device bus (for example, industrial bus used in specific industries).

4.4.4 Insertion / Removal of UICC

4.4.4.1 High Level Requirement

In some specific use cases it could be required to insert and remove the UICC by means of device handling procedures to be established by the host device manufacturer. However, some form factors (that is, soldered) may not allow easy removal of the UICC and other procedures may need to be considered.

4.4.4.2 Considerations

There are a number of reasons why the UICC may have a requirement to be removable - for example, upgrade by the end-user, the MNO, the device manufacturer or the service provider, and so on. For instance, when an embedded device is serviced for repair or a service provider changes its devices, service provider intervention may be required to move the UICC to the new devices.

If the user or the service provider cannot readily replace the UICC, this might require a removal/replacement process to be established by the device manufacturer identifying how such removal/replacement should be accomplished.[4]

4.4.4.3 Guideline

It is desirable that removal of the UICC under specific circumstances is allowed. Where such removal/replacement is not allowed by the user or the service provider, then the necessary procedure should be clearly defined by the device manufacturer.

[4] The considerations to accomplish this capability are currently being studied by the GSMA Embedded SIM project. Once the project output has been published the output will be available for review and subsequent updating of this section

4.4.4.4 Security Guideline

The embedded module shall detect the removal of a powered UICC and if possible terminate all radio connections / services authenticated by the (U)SIM application on that UICC. All temporary keying material related to this UICC should be deleted.

A practical way of preventing continued usage of previously authenticated connections after UICC removal would be to impose a constraint so that the UICC can only be installed or removed when the module battery is detached and power supply is disconnected. Alternatively, solutions might be considered which provide for a similar effect (for example, by enforcing shut-down of the embedded module following UICC removal

In some cases, there may be a requirement to associate a removable UICC with an embedded module in a 1-to-1 relationship, to protect a restricted subscription by ensuring that it will only be used to provide service to a particular module. Achieving such pairing is stipulated in ETSI TS 102 671 [28].

4.4.5 Remote Management of UICC

4.4.5.1 High Level Requirement

Due to difficulties and cost associated with physical access to the embedded modules and embedded devices – many of them in remote locations – there is a need for the UICC to be remotely managed.

4.4.5.2 Considerations

MNOs have a need to do occasional updates on the data on the UICC (as an example, updating of the preferred PLMN list).

The MNO owns the UICC and is the sole management authority for the card. In the future, it is possible that the MNO will designate (as part of the ETSI standards) a restricted area on the UICC in which access can be managed by a designated 3rd party but under the strict control of the MNO as permitted by Global Platform Card Specification v2.2 Amendment A.

4.4.5.3 Guideline

It should be possible to remotely manage the UICC.

Refer to ETSI TS 102 225 [29], ETSI TS 102 226 [30], 3GPP TS 31.115 [32], and 3GPP TS 31.116 [33] for guidance on the UICC remote management.

4.4.6 UICC Environmental Constraints

4.4.6.1 High Level Requirement

UICC should be sensitive to the environmental constraints of a host device, and vice-versa.

4.4.6.2 Considerations

The ETSI TS 102 221 standard [28] defines a set of operating temperature classes for UICCs:

- Standard range –25°C to +85°C (ambient temperature range)
- Temperature Class A –40°C to +85°C
- Temperature Class B –40°C to +105°C
- Temperature Class C –40°C to +125°C

The temperature class for the UICC should be aligned with the specified operating temperature range for the corresponding embedded module, when the UICC is hosted within the module. The UICC temperature class should not be less than the range for the module.

In cases where the UICC reader is not integrated within the embedded module, different constraints may however apply to both parts and for the UICC may very well depend on the UICC reader location in the device.

The environmental constraints apply to the set constituted by the UICC and its connector, when a connector is used to hold the UICC.

Within ETSI TS 102 671 [28], a range of classes has been defined based on the following environmental conditions:

- Humidity
- Corrosion
- Vibration
- Shocks
- Fretting corrosion

In addition, TS 102 671 classifies UICC according to data retention time and minimum number of supported memory updates, to cope with the long lifetime expectations of some embedded modules.

4.4.6.3 Guideline

To assure the quality of EM services, the UICC design needs to adhere to the environmental requirements defined by ETSI specifications in addition to the environmental specifications for the embedded modules.

In the long-term, it might be recommended that each specific vertical market defines a limited number of meaningful environmental profiles as a combination of class requirements for each of the above conditions based on the ETSI specifications.

5 Service Layer and Application Programming Interfaces (API)

5.1 General Guidelines

5.1.1 High Level Requirement

The services provided to applications by the embedded modules of all types described in section 4.1.1 are presented using industry standard APIs or other publicly available APIs, enabling the applications to be relatively agnostic to the specific Module used.

5.1.2 Considerations

Consideration needs to be given to the control and data plane application interfaces presented by the embedded module.

The control APIs used by embedded modules to present services to applications may include the AT command suite as defined by 3GPP, with vendor specific extensions where required, in addition to other interfaces. Specific services may use service-specific protocols to transfer associated data.

The control APIs and service-specific data transfer protocols supported by embedded modules reflect the total set of services and interfaces to peripherals available on the embedded module and can vary considerably (UDP/TCP/IP, packet transfer, connectivity mgt, SMS, GPS, GPIO, ADC/DAC, I2C, SPI, and other market vertical specific interfaces). Service layer capabilities are being standardized in ETSI TC M2M (for example ETSI TS 102 689 [4] and TS 102 690 [5]) and in TIA TR-50.

The application environments used by embedded devices are diverse. An application execution environment may be provided with local access to the control and data. In such architectures the application execution environments vary (scripting, JAVA, and so on) and the services API presented may therefore vary accordingly.

Developers, whilst using AT commands, should take the following into account:

- AT commands follow specific syntax rules.
- AT commands have been standardised across 3GPP oriented embedded modules enabling migration for example from 2G to 3G, but different AT command standards have been defined for WWAN technologies (ex. UMTS and cdma2000). Application developers must be aware of these differences when developing for multimode devices.
- Some AT commands have been extended upon customer and operator request to enable new devices and markets by module manufacturers. Application developers must be aware of mobile network operator and vendor specific AT commands, some of which may have duplicate functionality.
- Due to the 7-bit interface of AT commands, binary data such as Multilanguage SMS characters must be transported using hex encoding schemes.

5.1.3 Guideline

It is recommended that all embedded module types described in section 4.1.1 present services through the AT command interface or other interfaces, and use service-specific data transfer protocols to enable the use of device drivers and middleware on the host device.

In host environment where control-APIs exist, as such APIs evolve, an appropriate host device driver shall be provided with the embedded module.

5.2 AT Commands & Common APIs – industry benefits

Depending on the type of the host application and the application structure, the host application can interface with the embedded module through an AT command interface or an API. AT commands are more suitable for smaller microcontroller and are used broadly among more industrial oriented applications. API’s are more suitable for more powerful OS based environments and can be found in handheld mobile computing devices like PDA’s. An example of a well-established API oriented interface is the RIL (Radio Interface Layer).

5.2.1 AT Command Approach

EM module types A and C have implemented the 3GPP standard AT command interface as a means for an application on the host application processor to control access to the cellular network and retrieve status from the module.

The AT command interface is today used by the majority of industrial M2M applications. The AT Command interface has specific characteristics:

- A broad set of commands which can be combined to form specific functionalities. 3GPP standard AT commands are implemented in the majority of industrial embedded modules. These standardized commands are complemented by extensions as well as customer specific additions. Standardized multiplexers offer the support of multiple AT command interfaces. AT commands exist for all 3GPP oriented technologies.
- There are operator-specific and vendor-specific AT commands to support customer-specific requirements.
- AT commands have been proven to work with applications using a wide range of microprocessors, from very small microcontrollers with low processing power, up to very powerful microprocessors.
- AT commands are 7-bit ASCII characters.
- Each AT command bus may be in one of several states
- Command state
- Data state - The device cannot be accessed by AT commands in Data state
- Online Command state - Transition to Online Command state requires nonstandard in-band escape sequence

5.2.2 Common API Approach

EM applications that operate in application execution environments (Module Types B and D) can be written to common APIs. For some applications the usage of API’s can be an alternative to AT commands.

The extension of the use of common APIs as an alternative to AT commands in Module Types A and C provides a number of technical advantages.

A number of applications may directly access the module at the same time. These types of applications are not to be confused with IP-based applications which do not interface directly to the module, but instead use the IP-bearer provided. Examples might include:

- An application that monitors and reports on sensor values, sitting alongside another application that might provide a diagnostic or management function.
- A vehicle tracking application alongside a separate application that tracks a container on or within the vehicle.

Concurrent access of different applications to the module through AT commands would not be possible – the usage of a common API would make this possible. Furthermore the common API would have the following benefits:

- Programmability: the usage of common APIs would encourage the usage of standard programming practices for software developers
- Concurrent Access: the single common API can be used by multiple concurrent applications
- Data Model: many common API function calls can be used across the different radio access technologies whilst operator requirements can be built into the common API in a generic fashion
- Modality: the device can be accessed by API calls at any time, irrespective of the state of the device and multiple access calls can be issued at the same time
- Binary data support: binary data can be sent natively without first hex-encoding
- IP-based data interface: Point-to-Point protocol (PPP) not required
- OS interface: the device appears as an Ethernet network interface card or mobile broadband device and it can be configured to be always on if there is network connection (auto-connect). Connections will automatically resume when a device is restored from suspend/hibernate mode and TCP applications will only attempt to use a device if it is connected.

5.2.3 Context – Different Types of Common APIs

Within an embedded module, applications must run within an execution environment. The execution environment generally provides, at a minimum, the most basic services required to launch the application. APIs provide additional building blocks, in the form of functions and data objects that can be used by application writers to gain access to the device and network services required by their applications. An application is usually written in a high-level language. This application source code is compiled to a machine (or virtual machine) instruction set and/or packaged for installation into the device's execution environment using a set of tools, often referred to as the “tool chain”.

The combination of execution environment and tool chain is often called a “development framework”, or simply a “framework”. APIs can be designed to be independent of a framework, in which case they can be made available to application programmers in multiple frameworks. Other APIs are designed to take advantage of unique characteristics of a particular framework, and therefore become dependent on that framework. Furthermore, some APIs are limited to one framework or another by the fact that they are proprietary to a particular technology vendor.

A wide variety of high-level programming languages are available for EM devices, including C/C++, Java, Lua, and Python. In addition, a wide variety of APIs are available, and new ones are being developed all the time. An example set of portable, general-purpose APIs is POSIX (Portable Operating System Interface), which is commonly available on Linux-based devices and many real-time operating systems (RTOS). EM applications can be built directly on top of the POSIX APIs provided by the Linux-based EM device. In addition, specialized APIs (e.g., a location services API) that are not a part of the POSIX APIs can be utilized by applications running on a Linux-based EM device.

5.2.4 Services provided by a Common API

The common API exposed by the embedded module should consider making the following generic services available to the host application processor:

- Device connectivity service: Enables the host application processor to connect to the embedded module and to terminate the connection. In many cases there is no separation between the modem processor and the application processor, therefore this service is only required in some cases when there is a separate modem processor.
- Network access service: Enables host applications to scan for available networks, to register and attach to a selected network, set network preferences and parameters, and obtain information about the current serving network (MCC/MNC, roaming status, and so on.)
- Wireless data service: Enables the host to command the module to start and stop IP data sessions, configure session parameters (DNS, Mobile IP, and so on) and obtain data session statistics (for example IP address, data rate, session duration, total numbers of bytes transmitted and received); also provides for remote wakeup capabilities.
- Asset service: Provides a programmatic interface to assets which are accessible via input/outputs (I/Os), including:
    - General Purpose Input/Outputs (GPIOs) – sensors
    - Universal Asynchronous Receiver-Transmitter (UART) – short-range wireless (ZigBee, Bluetooth)
    - Inter-Integrated Circuit (I2C) – accelerometers, cameras, touch-screen displays, etc.
    - Secure Digital Input/Output (SDIO) – memory card, offboard WLAN
- M2M service layer: Provides access to the services provided by an M2M service layer such as what is being defined by ETSI TC M2M.
- Device management service: Allows the host application to obtain information about the embedded module (for example model number and hardware/firmware/software versions, support for circuit-switched/ packet-switched data and maximum data rate supported)
- Device management service: Allows the host application and/or the back end to obtain status information about the module
- UIM management service: Enables host applications to control and obtain information about the UIM connected to the device (set PIN, obtain ICC ID, and so on), and enables Card Application Toolkit (CAT) applications to interact with the module
- SMS service: Provides the ability for the embedded module to send and receive SMS messages under control of host applications
- Firmware management service: Allows the host application to control a firmware update of the module and to obtain information about available firmware versions
- Device triggering service: Provides the ability for applications (for example USIM application) to request the embedded module to perform an action (for example, stay connected until USIM downloads application or file update) or to collect the data from the embedded module (for example, environmental conditions like temperature)
- Location service: Enables access to the devices location. For example, access location via GPS coordinates.
- Wi-Fi handling and WLAN authentication service
- USSD service

- Device power management service
- Push service
- Asynchronous callback service: Notifies the device of events; reduces polling of device status.
- Access to vertical functionalities like eCall - Provides an advanced set of APIs that give access to the core in-band modem functionality.
- Security & Internet - Offers TCP/IP features (if not already supported on the application processor). Offers secure protocols such as https and other security extensions for increased security levels.

5.3 Embedded Mobile Device Software Configurations

5.3.1 Background

Embedded devices provide cellular network connectivity to sensors, smart meters, etc., to enable them to be remotely monitored and controlled

Applications running on embedded devices access the required device and cellular modem functionality via APIs.

Embedded device APIs share some functions with the APIs developed for cellular devices used in handsets and notebooks. However, embedded device APIs also have some important differences with handset and notebook APIs.

Embedded devices typically do not have user interfaces, so APIs for user interface functionality may not be needed.

Embedded devices need access to monitored entities, via device I/Os or short-range wired/wireless connections.

5.3.2 Components of an Embedded Device

- Assets: Entities that are remotely monitored and controlled as part of the embedded application (e.g. sensors, smart meters, trucks, etc.)
- Embedded device applications: Interact with network applications to provide remote monitoring and control of assets
- Embedded device API: Provides embedded device applications with access via APIs to asset data, cellular connectivity and other functions
- Modem: Provides cellular network connectivity to embedded device

5.3.3 Embedded Device Configurations

Embedded devices can be deployed in a number of different configurations.

Each has distinct requirements on where the application resides in the configuration and what API functionality needs to be exposed in each part of the configuration.

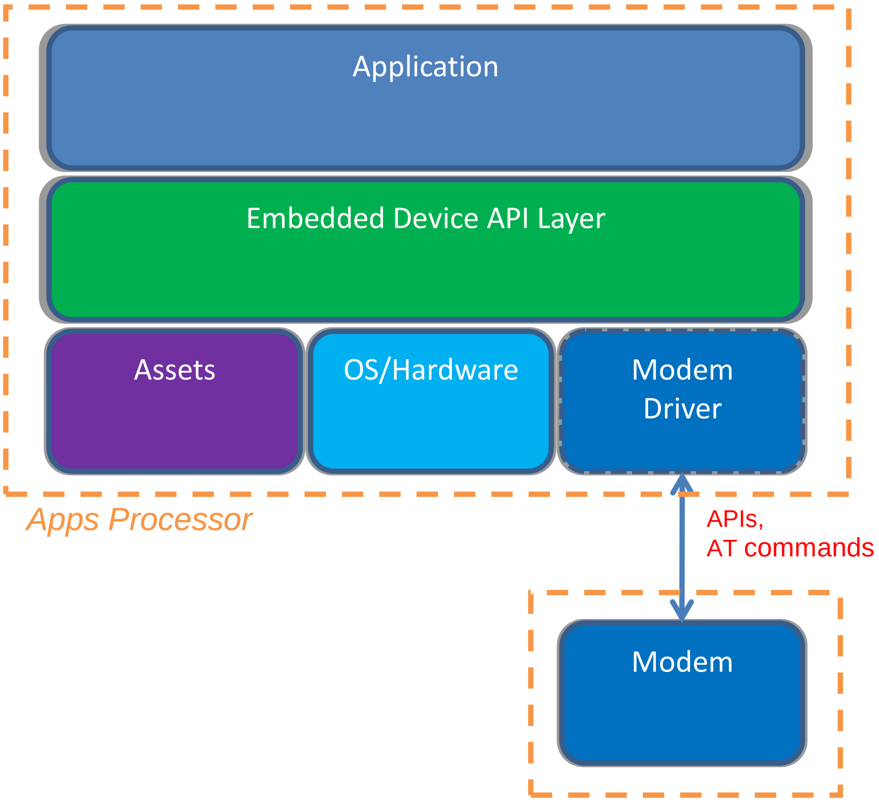


Figure 2: Applications Processor (AP) + Modem Configuration

In the “AP + Modem” configuration (), there are separate applications and modem processors. The “AP+Modem” configuration corresponds to module types A & C as specified in section 4.1.1.

The API functionality includes:

- Assets: accessible via I/Os, including
- GPIOs – sensors
- UART – short-range wireless (ZigBee, Bluetooth)
- I2C – accelerometers, cameras, touch-screen displays, etc.
- SDIO – memory card, offboard WLAN
- Operating System/Hardware: timers, threads, interrupts, memory allocation, etc.
- Modem driver: software layer that allows the embedded application to control the modem, via APIs or AT commands

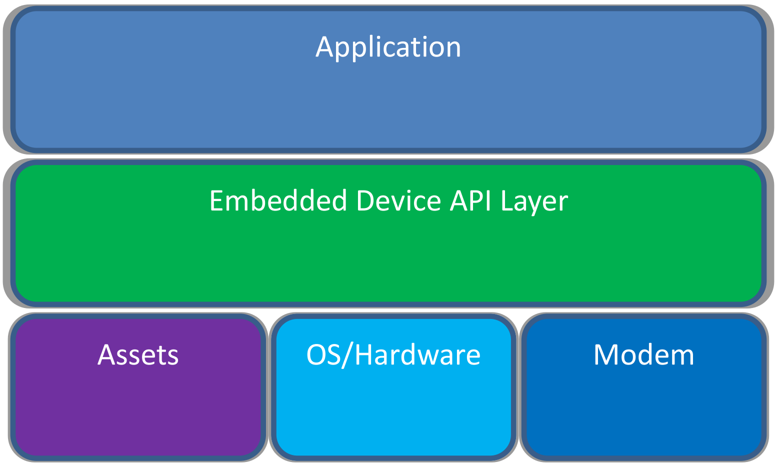


Figure 3: Standalone Configuration

In the standalone configuration (Figure 3:), the embedded device application and the cellular modem both reside within the module. Standalone configurations can result in lower module costs, since a separate applications processor is not needed.

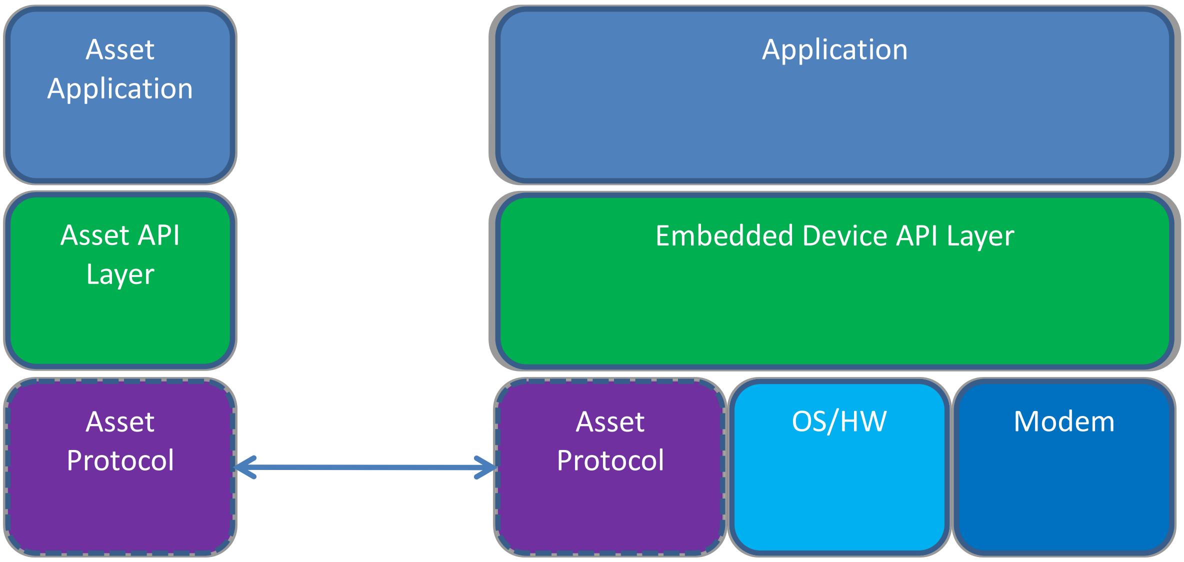


Figure 4: Gateway Configuration

In many embedded device deployments, the monitored assets are accessible over short-range wired or wireless connections. In the gateway configuration (Figure 4:), the embedded device must implement the necessary asset protocols and provide APIs to allow applications to access them, including

- Low-layer protocols (e.g., Bluetooth, ZigBee)
- Upper-layer protocols (e.g., IETF Constrained Application Protocol (CoAP), IEEE 11073 Optimized Exchange Protocol (OXP) for medical sensors)

Embedded devices that serve as gateways also perform certain functions on behalf of the monitored assets, e.g. “proxying” device management and service layer functionality

The gateway configuration is effective when the monitored assets have limited processing and communication capabilities

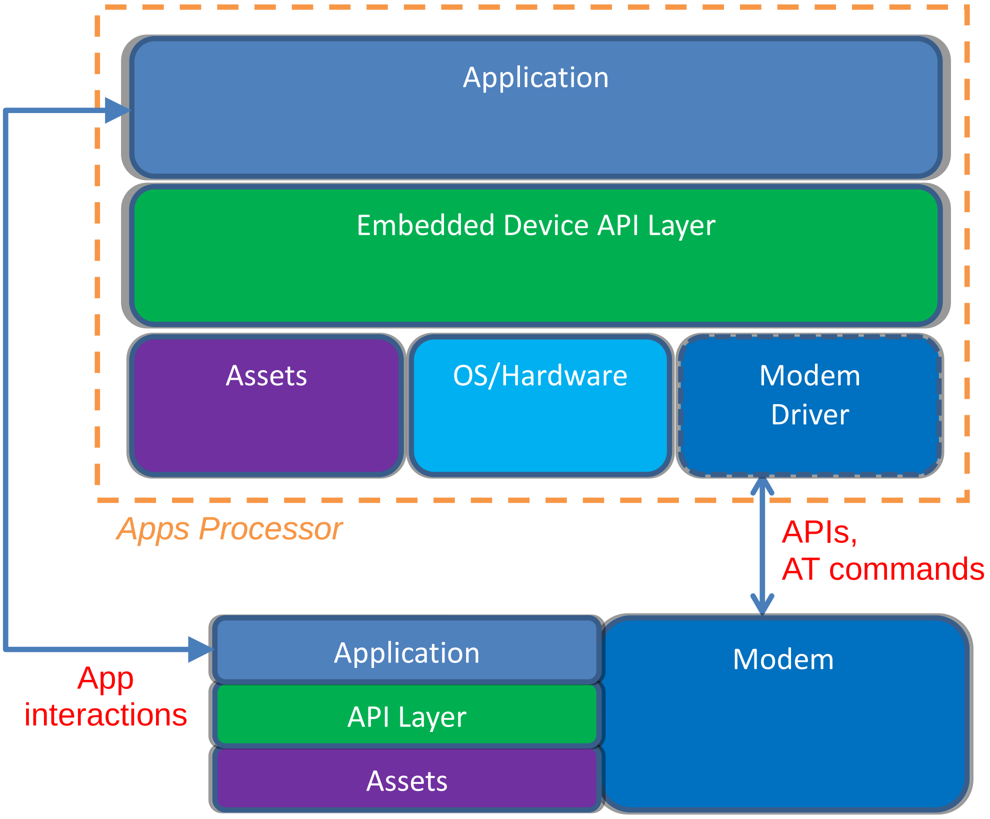


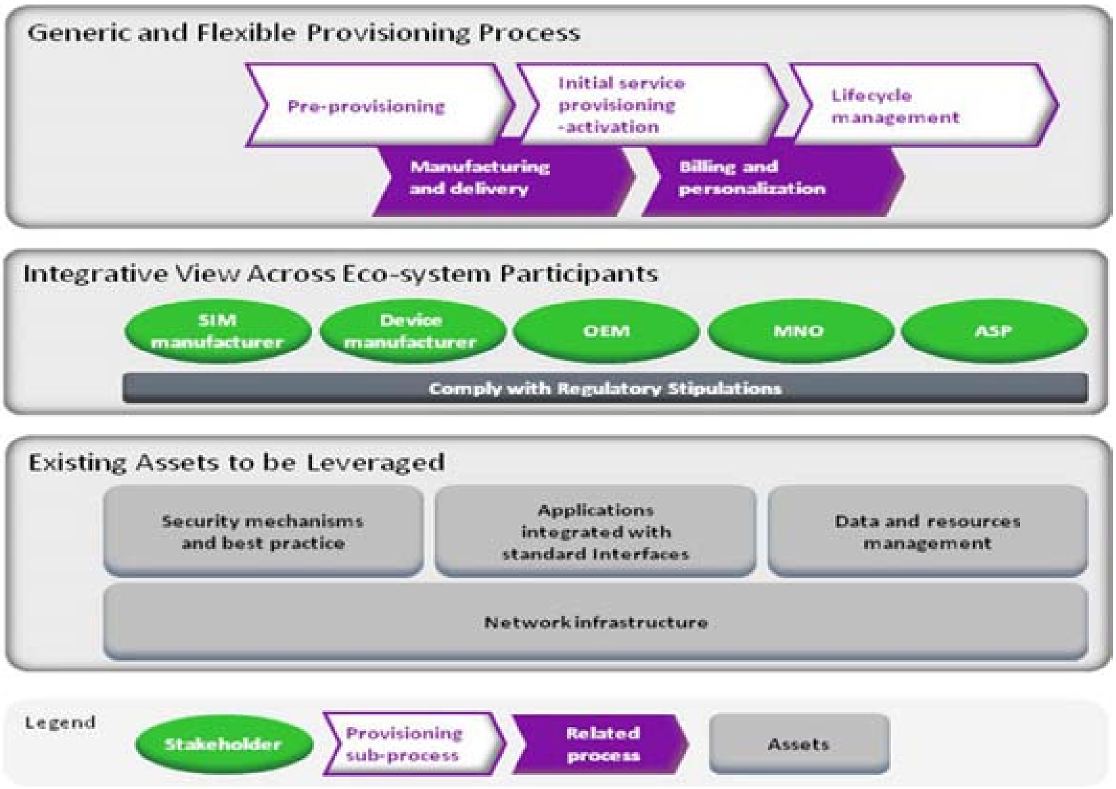
Figure 5: Intelligent Modem Configuration

In certain deployments where the Modem + AP configuration is used, it is necessary to run part of the device application on the modem processor (**Error! Reference source not found.**). This is usually done because some of the I/Os needed to access monitored assets are only available on the modem processor. The modem can be leveraged to reduce complexity towards the application. For example, peripheral wireless technologies such as short range can be hosted or controlled by the modem.

6 Guidelines for Provisioning and Management

Provisioning is the process by which an embedded device or a subscriber is enabled with the services required by that device or subscriber. These services can include, for example, access to packet data services, circuit data services, roaming restrictions, and so on. The services also include applications services that may be unique to the device or vertical in question – for example, telematics, metering, and so on.

An example provisioning process flow chart below outlines typical steps for an embedded device or service. The roles and responsibilities in the flow chart are illustrative and do not imply a general recommendation; as these are likely to differ per geography and/or vertical market.



Generic and Flexible Provisioning Process
Pre-provisioning
Initial service provisioning -activation
Lifecycle management
Manufacturing and delivery
Billing and personalization
Integrative View Across Eco-system Participants
SIM manufacturer
Device manufacturer
OEM
MNO
ASP
Comply with Regulatory Stipulations
Existing Assets to be Leveraged
Security mechanisms and best practice
Applications integrated with standard Interfaces
Data and resources management
Network infrastructure
Legend
Stakeholder
Provisioning sub-process
Related process
Assets

Figure 6: Key requirements for EM Provisioning Process

6.1 Provisioning Aspects

Three main aspects of provisioning are described below.

6.1.1 Pre-provisioning

Pre-provisioning of service capabilities allows a device and its associated service to be tested prior to distribution to reduce dead-on-arrival problems and customer service issues at the time of first use. Pre-provisioning to allow non-commercial testing prior to distribution can avoid these problems.

Pre-provisioning involves inserting the UICC in the device, having the UICC data (IMSI, authentication data, and so on.) provisioned in the network and service activation for the device/subscriber.

6.1.2 Initial service provisioning:

When the embedded device reaches the end-user, there may be service options to be chosen depending, for example, on the particular vertical market, the choice of the end-user or location of use. For example, a smart meter could be deployed in any location chosen by the utility, but once deployed the utility may want service for that specific meter to be limited to the location of first use. Therefore, there is a need for an initial service provisioning related to how the device is to be first used.

6.1.3 Life-Cycle Management

There may be a requirement to modify the services used by the embedded device over time. For example, additional services may be made available and/or chosen by the end-user. Therefore, there may be a requirement to update service options. In some cases, it may be necessary to make changes on the UICC – for example, change of the PLMN list on the SIM, change SMSC address or add/update SIM applets.

There are a number of key requirements for the provisioning of embedded devices (see Error! Reference source not found.**)**. The provisioning process needs to be standardized, automated and instant, and involve minimal manual intervention**.** This requirement applies specifically for the communications services used by a device, and may also apply to the applications services used by the embedded device.

In the initial phase of the EM market's development, existing provisioning processes should be reused as much as possible. This approach enables synergies with the underlying infrastructure environment and applications. In addition, it is important to take a multi-stakeholder view of the provisioning process to minimise implementation challenges.

An example provisioning process flow chart below outlines typical steps for an embedded device or service. The roles and responsibilities in the flow chart are illustrative and do not imply a general recommendation; as these are likely to differ per geography and/or vertical market.

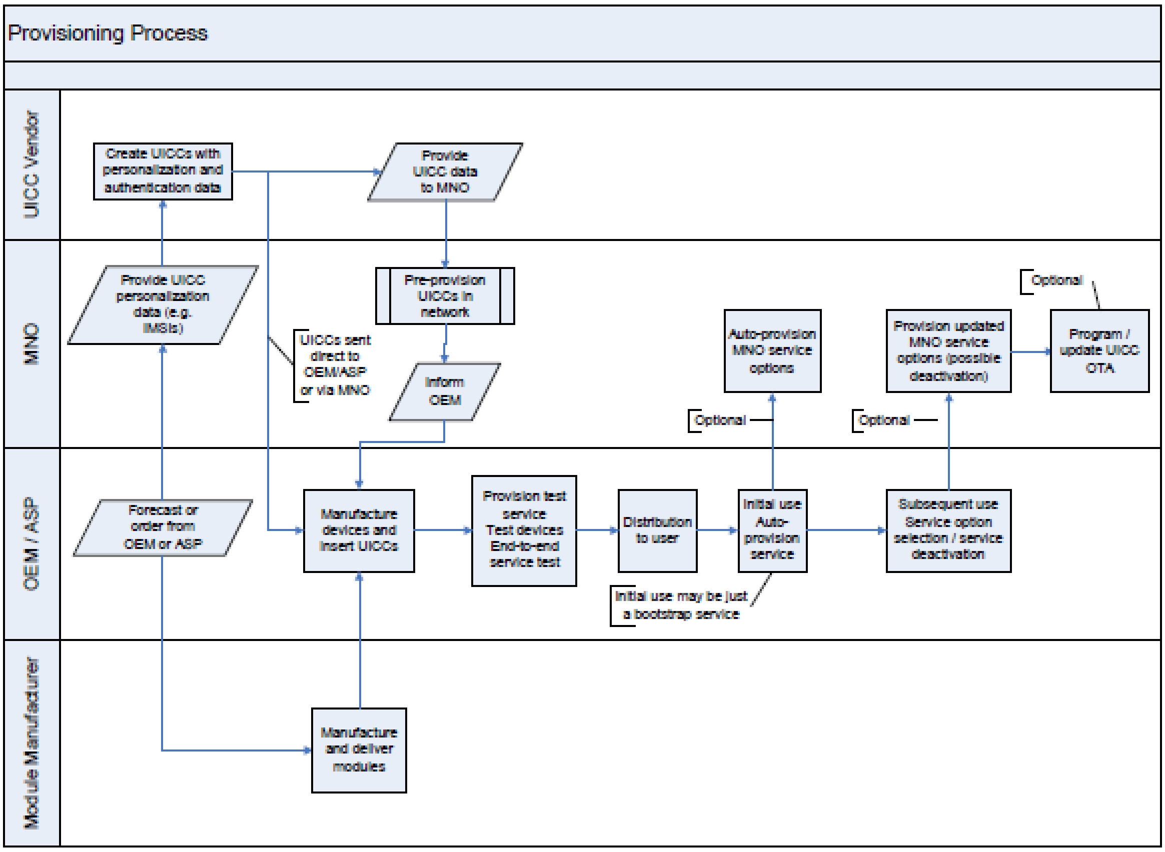

Provisioning Process
UICC Vendor
MNO
OEM / ASP
Module Manufacturer
Create UICCs with personalization and authentication data
Provide UICC data to MNO
Provide UICC personalization data (e.g. IMSIs)
Pre-provision UICCs in network
UICCs sent direct to OEM/ASP or via MNO
Inform OEM
Auto-provision MNO service options
Optional
Provision updated MNO service options (possible deactivation)
Optional
Optional
Program / update UICC OTA
Forecast or order from OEM or ASP
Manufacture devices and insert UICCs
Provision test service Test devices End-to-end service test
Distribution to user
Initial use Auto-provision service
Subsequent use Service option selection / service deactivation
Initial use may be just a bootstrap service
Manufacture and deliver modules

Figure 7: Provisioning Process Flow Example

In this chapter, the main guidelines are described for the provisioning and management of EM Devices and their associated services.

The chapter is structured in several sections:

- Guidelines for pre-provisioning of embedded devices
- Guidelines for initial service provisioning
- Guidelines for UICC provisioning and management
- Guidelines for embedded device management
- Guidelines for network management and optimisation

6.2 Pre-provisioning

6.2.1 High Level Requirement

To minimize problems at the time of initial use, it should be possible for the embedded device to be pre-provisioned with service to allow the device and its associated service to be tested before deployment of the device to the field.

6.2.2 Considerations

Testing may occur in a location or country that is different from the place of final deployment and pre-provisioning must take this into account. For example, a navigation device that is destined for use only in Europe may be manufactured and tested in Asia. Although the service profile for the deployed embedded device may include roaming restrictions outside of Europe, the pre-provisioning would not have such limitations.

Testing for one kind of vertical may vary from that of another vertical. For example, different services or volumes of traffic may be required for different verticals. Consequently, any pre-provisioning needs to be flexible to allow different usage patterns across different verticals.

The pre-provisioning related to pre-test of the embedded device should be bounded to avoid fraud. For example, pre-provisioning may be limited to a certain volume of data, certain locations of use, or certain times.

6.2.3 Guideline

Embedded devices should be pre-provisioned to enable end-to-end testing before deployment. This pre-provisioning should be configurable to account for the service requirements of the vertical in question.

6.3 Initial Provisioning/ Bootstrapping

6.3.1 High Level Requirement

Some embedded devices require an initial boot-strap level service to be provisioned so that a device can communicate enough to allow longer-term service to be provisioned. For example, consumer electronics embedded devices may need to be provisioned for sufficient communications capability for the user to reach a service selection page to select longer or additional service options. Another type of embedded device (for example, a telematics device) may be configured to reach a central server which will then configure the device remotely with service options (for example, E-Call, B-Call options, roaming options, and so on.)

6.3.2 Considerations

Initial service should be available at any time or location, regardless of service restrictions that might apply to the subscribed service. The type of initial service may vary by vertical. In general, the service is provisioned and managed by the MNO and/or the ASP on behalf of the MNO. The module should not limit the initial service in any way.

6.3.3 Guideline

Embedded devices should be provisioned with an initial service that allows for the end-user to select a longer term service, or that allows a service provider to configure the device remotely and also provision an updated service.

6.4 Initial UICC Provisioning

The key requirements and considerations for the initial UICC provisioning are currently under development by the GSMA Embedded SIM project. Once the project output has been approved, it will be available for review and subsequent updating of this section.

6.4.1 High Level Requirement

It shall be possible to select the initial MNO and securely provision the necessary network access and service subscription either before or after the delivery of the embedded device to the service provider or the end-customer as deemed necessary by the service provider.

It should also be possible in some vertical markets to allow for the selection of a new MNO (upon contract termination) and the secure provisioning of the new network credentials and service subscription using remote provisioning facilities.

6.4.2 Considerations

Flexible provisioning of the UICC credentials is necessary to allow the service provider with flexibility in the selection of the initial and subsequent MNO in a multi-MNO market. In addition, providing the service provider and the end-customer with the flexibility to select the MNO of choice, the capabilities should allow for service activation to occur after the subscription has been agreed with the MNO and the network access confirmed.

The considerations to accomplish this capability are currently being studied by the Embedded SIM project. Once the project output has been published, it will be available for review and subsequent updating of this section.

6.4.3 Guideline

The MNO should provide the ability to remotely update the SIM in accordance with the needs of the service to be provisioned. It should be possible to trigger these updates remotely and automatically as the service parameters are updated.

More specific Guidelines may be identified once the Embedded SIM project output becomes available.

6.5 Device Management

6.5.1 High Level Requirement

Tamper-resistant management of the embedded device should be provided independent of the service (if any) executing on the device. Device level firmware upgrade should be made available.

6.5.2 Considerations

There is need to provide a standards-based approach, for example, as supported through the Extensible Management framework customisable by device vendors with access control.

Key considerations with respect to device management include:

- Bootstrap Provisioning, remote maintenance and reporting of configuration data
- Device diagnostics and fault management, including device integrity checking and reporting
- Application and Non application software/firmware update (FOTA) and management including:
    - Hardware and Software Inventory
    - System configuration
    - Device Health, including status of post-FOTA application integrity checking
    - Performance
    - Error and warning alerting and monitoring
    - Temperature monitoring and management
    - Power Management
    - Network usage
    - Lock and Wipe
    - Task Scheduling

In addition, the following M2M specific device management requirements are currently under consideration at the Open Mobile Alliance (OMA):

- Extension of the OMA Device Management (DM) Specifications in terms of protocol, management objects, and other network bearers to support restricted capability devices;
- Investigation of existing light-weight protocols currently in use or being developed in other standards bodies for the purpose of M2M connectivity. If none are applicable to OMA DM requirements, development of a new lightweight DM protocol to support these M2M capability-limited devices will be pursued.
- Continuation of work on the OMA DM gateway and extension of the requirements necessary to address M2M networks;
- Addressing OMA DM Security related issues.

6.5.3 Guideline

It is recommended that the remote management interface of the embedded device uses an open-standard based extensible device management framework such as OMA DM.

6.5.4 Firmware Upgrade

6.5.4.1 High level requirement

For certain use cases it is necessary to be able to update the software of the EM devices remotely. This can include application software (embedded applications running on the module – for example Java, Python or compiled C) in addition to the firmware of the module.

6.5.4.2 Considerations

In general the firmware update process consists of a client that executes the update and a server which delivers the firmware.

There are mechanisms which allow the initiation of the process by means of the network.

Common remote firmware update mechanisms are based on the Open Mobile Alliance (OMA) Mobile Device Management (MDM) standard and are often referred to as FOTA (Firmware over the Air). Within this framework there are specific proprietary extensions offering additional features. Different degrees of features are available in addition to a range of server solutions by various vendors.

An alternative way to perform a firmware update of the module is via the device in which the module is embedded. In this case the device executes the standard update process by updating the module via the control interface.

The specific use case of the device determines the implementation of the type of the update solution. The update of embedded applications running on the module is generally included in the environment used (for example. Java, compiled C, Python).

For the update of the module firmware there are various options – from simple update of the firmware to advanced device management.

6.5.4.3 Guideline

Since embedded modules are often operating in a complex eco system with many players and different roles, the responsibilities of the involved parties including the process for updating the firmware must be defined.

When updating the firmware it is essential that all approvals of the device are maintained. A change of firmware may lead to re-testing and could lead to the re-certification requirement of a host device prior to the rollout of a firmware change.

A long-term objective is to streamline the processes for compliance, and avoid re-certification of a host device, shifting the burden of re-testing and re-certification to the EM module.

6.5.4.4 Security Guideline

⚠ Appropriate security measures must be deployed to prevent unauthorized or insecure implementations of the firmware update mechanism.

6.6 Application Development Enablers and Control

6.6.1 High Level Requirement

Service and application providers need to develop and deploy sophisticated services that are agnostic to the bearer connectivity/transport and the embedded module deployed.

6.6.2 Considerations

This is a considerable challenge for embedded devices because of the diversity of the application domains (unlike Notebook and PC like environments which are standardised). However, there is a considerable advantage in enabling common applications to be utilised, enabling faster time to market and more intelligent component-based embedded applications to evolve.

The APIs should be considered with respect to the language, frameworks and OSs the upper layer applications are deployed on. As the services and interfaces offered on the module increase, and vary to meet the use cases of vertical segments, the availability of standard APIs for drivers and so on becomes a critical factor in enabling a rich set of application enabling ingredients.

The existing trend in home gateways, mobile handsets and mobile internet devices to use a JAVA-based applications environment might be considered, as it isolates the applications from the OS and specifics of the embedded device. Other considerations could include OSGI (Open Services Gateway Initiative), WRT (Web Runtime Environment), MIDP (Mobile Information Device Profile), IMP-NG (Information Module Profile – Next Generation), BREW Mobile Platform, among others.

6.6.3 Guideline

It is recommended to use application deployment and runtime environments that are OS agnostic.

6.7 Charging

6.7.1 High Level Requirement

Embedded devices represent a new category of subscriptions that in most cases need to be handled separately from a charging perspective. Efficient and versatile charging data treatment functionality already available in mobile networks makes it possible for MNOs to package their service in a way that suits the needs of these customers. In most of the vertical sectors the embedded devices will form large groups that can be managed together for charging. The processes should be optimised to allow this type of grouping to minimise the effort on charging data treatment.

6.7.2 Considerations

Current mobile networks support advanced features for time and/or volume based charging in diversified charging schemes that support the services being offered. The network operator can monitor the network closely and can collect information for post processing purposes and/or for immediate control actions in near real-time. These features also enable good network usage analysis, which can be used for optimization, as progressively more embedded devices enter the network.

It is likely that the connectivity service for large groups of embedded devices will be provided to a single customer, for example, companies that provide remote metering services to utilities. In many cases the customer, such as the remote metering company, will not be interested in the charging statistics of a single device, providing it is behaving normally. This could mean that information collection and control is applied to a group of devices. However, in addition to group treatment, it may be necessary to collect information and control individual embedded devices belonging to one of these groups. Due to the specific nature of embedded devices communication, the relation of signalling may be high to user data, and it is essential to be able to handle information on signalling along with user data.

While the existing charging standards support a versatile set of functions that can be used for services specific to embedded devices, it is worth noting that some of the more advanced charging concepts may require further 3GPP standards efforts.

6.7.3 Guideline

It is recommended that charging for groups of EM devices is enabled on mobile networks, to achieve efficiency in data treatment functionality.

3GPP specifies requirements for such charging data treatment in TS 22.115 [31]; other standards for charging groups of devices together are currently under development and should be taken into consideration by EM service providers.

7 Guidelines for Testing and Certification

7.1 Introduction and Scope

This section is intended to provide guidance on the testing and certification for embedded devices with fully integrated 2G/3G mobile radio capabilities. It is not intended to detail specific test cases, but rather provide a high level approach to specifying which suite of test cases should apply for module testing and which should apply to the host device product.

Integrating 2G/3G embedded modules into non-traditional mobile devices triggers a test and certification program that may place a significant schedule and cost burden on the vertical market device manufacturers to the extent that this becomes a barrier to entry for embedded devices across vertical market segments.

To promote the proliferation of embedded devices, the test and certification process must be optimised to provide a faster time to market with lower costs without compromising the end performance and safety of the network.

One of the most significant challenges associated with the test and certification of embedded devices is dealing with the multiple device types offered across different vertical markets.

This section offers guidance in managing the certification of embedded devices and the associated variants offered across different vertical markets under the Machine to Machine (M2M) umbrella.

The chapter is structured in several sections:

- Overview of certification requirements
- Recommended approach to certification
- Recommendations for embedded device RF exposure testing and reporting
- Guidelines for managing certification of embedded device variants
- PTCRB approach to embedded device test and certification
- Embedded device test positions and modes of operation for radiated performance
- Radiated performance requirements for large form factor host devices

7.2 Overview of Certification Requirements

Certification requirements for an embedded device fall into three distinct categories:

- Regulatory Certification
    - Depending on the vertical market multiple regulatory agency approvals may be required
    - Regulatory certification may be required in multiple markets with each market having its own regulatory body and approval process
    - Regulatory approval of module plus host device is required. Pre-certified modules can significantly reduce the cost and time to market of the embedded device certification
- Industry Certification
    - Telecom Industry specific certification (GCF (Global Certification Forum), PTCRB)

  - Vertical industry specific certification (for example, automotive)
- Operator specific certification

Operator specific certification is required for host devices and modules. A pre-certified module can significantly reduce the cost and time to market of the embedded device certification.

Embedded devices may be required to be certified and offered across multiple network operators

The following figure provides an overview of the certification requirements for an EM device

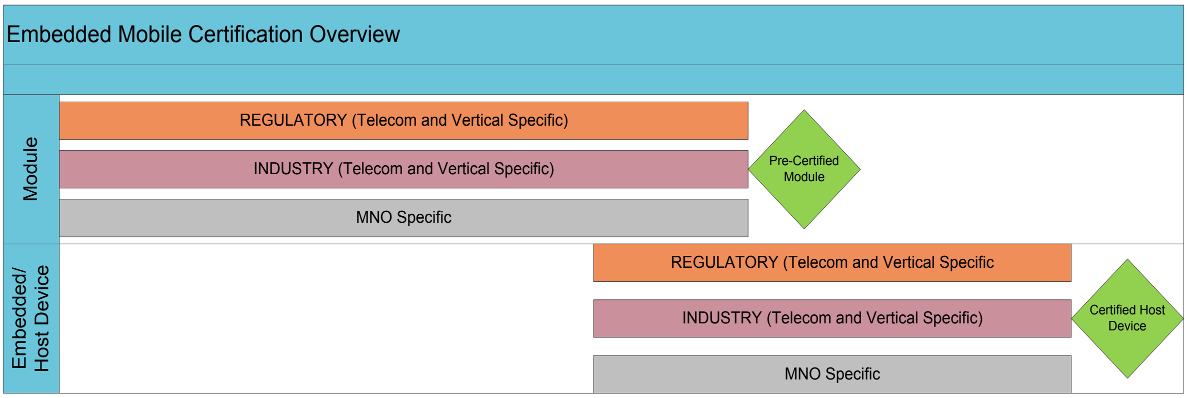

Embedded Mobile Certification Overview
Module
REGULATORY (Telecom and Vertical Specific)
INDUSTRY (Telecom and Vertical Specific)
MNO Specific
Pre-Certified Module
Embedded/ Host Device
REGULATORY (Telecom and Vertical Specific
INDUSTRY (Telecom and Vertical Specific)
MNO Specific
Certified Host Device

Figure 8: Certification Overview

7.2.1 Global Certification Forum (GCF)

GCF offers two defined paths to a certification. Certification of devices (for example handsets, modules...) requires a full evaluation. For the certification of ‘connected devices’ (devices embedding 3GPP radio modules previously GCF certified, for example notebooks), GCF has defined dedicated guidelines specifying a ‘fast track’ towards a certification.

To participate in the scheme, manufacturers must first become a member of GCF. They must also become Quality Qualified, which involves a self-declaration that they have a recognised quality assurance programme in place for their design, development and manufacturing processes.

In addition, manufacturers are required to indicate that they possess, or have subcontracted for, the skills and means of test to perform the self-assessment of their new product's conformity with the relevant GCF certification criteria. The requirement is that the test lab is ISO17025 certified. This stage is referred to as Assessment Compliant.

When starting a device certification, the implemented device functionality is identified according their PICS/PIXIT table and the applicable criteria and conformance test cases are selected using the GCF Database Certification Criteria (DCC). This can be done by the vendor itself or by an external test house.

If valid test results are available from previous testing or other (ISO17025) sources, no new testing is required. If the device embeds a certified module, the module is referenced and the dedicated guidelines are used for identifying applicable test criteria. Please note, that a GCF certified module can be used for three years until it needs either to be re-certified against the latest GCF-CC (Certification Criteria) version or replaced by a newly certified module.

Once a new product has successfully met all the relevant certification criteria, the manufacturer can declare it as having achieved the terminal certified status and can submit it to GCF for registration. The appropriate documents to complete are provided by the GCF website during the registration process. If the device including a GCF certified module is embedding several different types or brands of modules, each module needs to be registered on the website separately, together with the host device.

The manufacturer is also required to maintain appropriate traceable documentation to support this declaration in a ‘Compliance Folder’. This documentation is kept updated for every device update and can be inspected by operators under bilateral conditions.

GCF CC are continually updated with new or modified test cases and a product must be certified within the period for which a specific CC version is valid. Timing is vital, especially when considering the schedule for integrating an already GCF certified module into a device and the start of actual testing with a service provider. Typically, a carrier will request certification to the latest GCF CC.

GCF approval requires both conformance lab testing and Field Trials. Whereas the Field Trials for full certification include testing in 5 networks, the Fast Track Field Trial for a ‘Connected Device’ (for example a mobile enabled smart meter) is limited to a one-day confidence testing done stationary on one live network.

When a product is approved to a particular version, changes made to that product can also be approved to the original version, unless new features are added then the product must be approved to the current version.

An overview and dedicated guidelines are available at:
http://www.globalcertificationforum.org

7.2.2 PTCRB

PTCRB is the North American operators’ certification body for GERAN, UTRAN and E-UTRAN devices. The purpose of the PTCRB is to provide the framework within which device certification can take place for members of the PTCRB. This includes, but is not limited to, determination of the test specifications and processes necessary to support certification of GERAN, UTRAN, and E-UTRAN devices. PTCRB is also responsible for generating input regarding testing of devices to standards development organizations.

PTCRB procedures and requirements are specified and/or defined in PTCRB’s PPMD (PTCRB Program Management Document) and NAPRD03 (Permanent Reference Document).

Embedded modules are certified in the same manner as a handset. This allows for greatly reduced testing of products embedding certified modules. The certification process is initiated by registering as a “Manufacturer-Observer” via the PTCRB website (www.ptcrb.com). Then, the embedded module vendor submits a certification request via the PTCRB database. At the time of the request, the vendor selects a PTCRB accredited lab to manage the certification. The version of NAPRD03 is established based on the completion date of testing, and includes all applicable tests approved and published in one of the two most recent versions of NAPRD03.

Devices integrating embedded modules initiate the certification process by submitting a certification request via the PTCRB database. The vendor will select a PTCRB certified lab to manage the certification. The integrated device is subject to testing against the same version of NAPRD03 as the embedded module was certified against. However, only those areas not previously tested during the module’s certification and those areas changed or impacted by the integration of the embedded module are tested, so much of the module’s testing is leveraged. The embedded module, hardware and software, must have been certified within the last 3 years. This is to ensure that modules are reasonably up to date and functional with the latest network features.

7.2.3 Mobile Network Operator, (MNO) Testing

Mobile network operator approvals are typically mandated to ensure the quality of mobile devices operating on the network and maintain a high level of wireless service for customers. In order to accomplish these goals many MNOs may each require a plethora of internal and regulatory/industry tests for device approval resulting in complex process flows and lengthy certification schedules. If possible, it is desirable to arrange the test process in a parallel fashion in order to minimise the approval phase costs and duration.

These tests may include regulatory/industry tests such as those conducted by the PTCRB, GCF, FCC, etc, module vendor development and regression testing, OTA (over the air) tests, MNO specific network feature tests, and integrated platform tests such as TRP/TIS and communication clients. Many of these tests are particularly applicable to the embedded module vendor and are undertaken in the module development test cycle. For instance, a module may be taken into a MNOs test process to begin MNO specific test cases while ongoing vendor development and regression testing continues. In the US, for example, when the embedded module is judged to be sufficiently mature module IOT testing at infrastructure vendor labs may be started in parallel with MNO specific tests, and module PTCRB certification. This phase might be followed by OTA testing, FCC submission for the final module hardware, and the formal service provider qualification process.

When a module reaches a stage where it is ready for interoperability testing, then testing with a target device platform may begin. For instance, as the module interoperability testing at infrastructure vendor labs begins, a parallel testing effort with IPT TRP/TIS and the communication client can be initiated.

The recommendation endorsed by the GSMA Test & Certification work stream with regards MNO OTA performance testing is that for 3G devices, the values recommended and agreed by the 3GNBK group be used as a baseline for M2M Devices. A future work item may be considered to investigate and define further values for 2G and 2.5G defining a common test denominator from various MNOs and incorporate the set into regulatory/industry testing process. This would benefit the entire test community by extracting the common set of tests to be performed once (or until passed), thus eliminating the need for these test cases to be repeated by each MNO.

Testing required for an MNO approval typically includes standardised tests specified by GCF and/or PTCRB for the independent module and embedded device. In some cases, operators focus only on testing of the final application, so module testing is not always mandatory, accelerating time to market for a final application. MNOs may also specify a set of mandatory and optional device requirements that are specific to its own network implementation. The majority of MNO specific tests usually pertain to the radio requirements and therefore impact the embedded module.

The module vendor will typically address them directly during Stand-Alone Module Testing (SAMT) as described in section 7.3.1.1. A subset of MNO specific device requirements may be applicable to embedded device testing (EDT). Guidance for EDT is provided in section 7.3.1.2.

MNO specific requirements for data devices may include, but are not limited to, data rate support, band support, transmit power class, radiated performance (TRP/TIS), self-interference (all channel evaluation), other requirements unique to a particular MNO network, and communications drivers.

It is generally recommended that vendors work with MNOs to understand and share technology roadmaps to ensure that data devices can meet evolving network standards and feature rollouts in a timely manner. MNO specific requirements for radiated performance and self-interference should be solicited as early in the integration process as possible so that any delta from published standards can be identified and managed as part of the total design and test process.

7.3 Recommended Approach to Certification

The recommended certification approach is to divide the testing into three distinct phases:

- Phase 1: Stand-Alone Module Testing (SAMT)
- Phase 2: Embedded Device Testing
- Phase 3: Embedded Device Variants

Dividing the testing into three phases allows for the majority of the MNO testing to be performed at the modular level by the experienced module provider, thereby reducing the burden on the embedded device integrator to a limited set of MNO tests at embedded device testing level. Dividing the testing into three phases allows for module certification independent of a host platform. The benefits of three-phase testing are especially important for testing and approving a module for use in multiple platforms, such as in the case of vendors who typically offer a 'family' of devices.

Following module approval, it is then only necessary to perform a small suite of tests – those related to the integration of the module (for example, radiated performance, radiated spurious emissions, and SIM electrical testing) – to validate the embedded device.

7.3.1 Proposed Test Procedure

7.3.1.1 Stand-Alone Module Testing, (SAMT)

Stand-Alone Module Testing (SAMT) is defined as testing a module when it is mounted into a test jig that allows for connection of power, control signalling and RF coax (antenna or cabled).

During this testing phase, tests are performed specific to the module and independent of the host platform. Areas for testing include, but are not limited to, the following:

- Protocol compliance testing
- Conducted RF performance and compliance testing (sometime referred to as cabled or non-radiated RF testing)

As these tests are completely independent of the host platform, they can be performed using only the module and a test jig. This allows for completion of the majority of the test suites without the need to wait on the host platform, which is going through its own design and development at the Device Manufacturer. Furthermore, at this stage the module manufacturer is not limited to testing with a small number of vendor-supplied platforms.

7.3.1.2 Embedded Device Testing (EDT)

Embedded device testing (EDT) is required to specifically address those tests that are specific to the integration of the module into the embedded device. Potential testing includes, but is not limited to, the following:

- Radiated Performance Testing
    - Radiated test cases presented as GCF-CC and PTCRB certification requirements for example, Radiated Spurious Emissions
    - Equivalent Total Isotropic Sensitivity (TIS) and Total Radiated Power (TRP) tests currently defined for handset devices. These tests and associated CTIA procedures cannot be readily applied to traditional M2M devices and therefore other test methodology needs to be applied.
- UICC/SIM electrical test cases presented in GCF-CC and PTCRB certification requirements.

- Mobile Network Operator drive testing (if required)
- User experience:
    - Client software interoperability
    - Installation
    - Initial registration
    - Connection configuration and management
    - Software driver interactions

7.4 Recommendations for Embedded Device RF Exposure Testing and Reporting

RF Exposure assessment is mandated by Regulators in a number of countries including US, Europe and Japan. RF Exposure compliance is also strictly monitored by the MNO to ensure that their customers are given accurate information on actual RF exposure values and any associated restrictions on use of the product.

For those vertical markets (for example, healthcare and consumer) defining “body worn” or “near body” EM devices, attention must be given to design, test and certification in accordance with Specific Absorption Rate (SAR) requirements.

For additional information and guidance on RF Exposure please refer to the FCC OET website as the US has the most stringent regulations on RF Exposure.

7.5 Managing Certification of Embedded Device Variants

There are a number of existing and emerging embedded devices in the vertical market segments that would benefit from 2G/3G embedded connectivity. These devices come in different form factors and levels of complexity. When offering WWAN as a feature across multiple product lines there is a risk that certain embedded device configurations will have an impact on the performance of the embedded module and network. The overall impact could manifest itself in poor end user experience (for example, coverage and throughput) and degradation in network efficiency. A barrier to proliferation of embedded devices would be a requirement for all device vendors and MNOs to have to test and certify all configurations.

One of the tests that will be required for embedded devices is an assessment of radiated performance in accordance with established sensitivity and transmit power requirements defined by the MNOs for different device categories.

Device compliance with minimum radiated performance requirements is essential to ensure a sufficient quality of service and performance. However, it is a costly and time-consuming process. Each embedded device potentially has a different RF emission profile. This creates the possibility of new interference sources within the embedded device coupling into the module receiver band. As a result of new interference sources, a fresh evaluation of radiated power and receive sensitivity may become necessary.

7.6 Considerations for Embedded Device Testing

Companies looking to certify embedded devices should ensure that they have a well-defined test plan in place prior to beginning actual testing. This may involve seeking out the right balance of partners to supplement their own understanding and appreciation of the Test and Certification requirements. Here module integrators, module vendors and test houses may be able to provide the advice and guidance required.

Considering the varied nature of M2M devices, this document does not attempt to provide practical advice on specific testing orientation. Instead, this document describes the high level end-to-end process.

Module manufactures will gain industry certification via certification bodies such as PTCRB and GCF. Use of approved modules for integration into a host device is recommended. By using an approved module, the additional testing that is required of the integrated device is reduced to the components which may be affected by the new module environment. The delta in approval testing that will be required to pass certification tests will need to be "calculated". It is therefore recommended that newcomers to the field seek out partners to assist them.

Approved products (hosted devices) are likely to require further operator network testing to ensure that they meet network requirements.

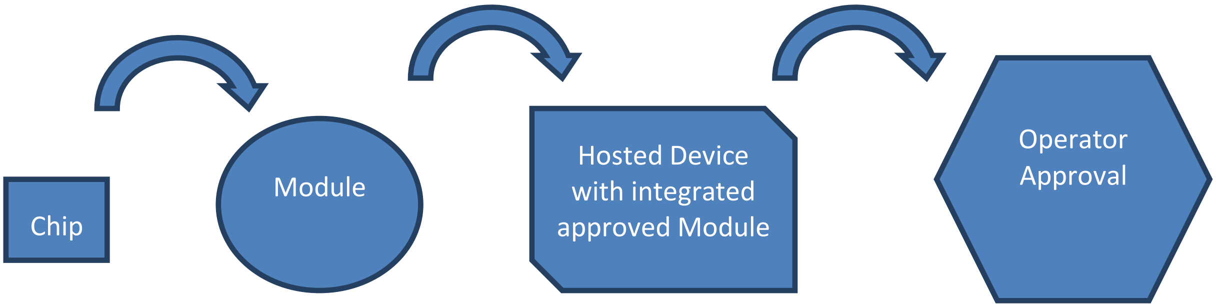


Figure 9: Embedded Device Testing

7.7 Radiated Performance Requirements for Large Form Factor Host Devices

For large form factor devices (for example, cars, automatic teller machines etc.) the standardized TIS and TRP test procedures cannot be applied. As the radiated performance of the host device with embedded antenna and embedded module is critical to in-service end performance and network efficiency, it is important to make an assessment of the radiated performance at host level using other methodology

Radio performance of large form factor host devices can still be evaluated in terms of free-space TIS ([dBm]) and TRP ([dBm]) parameters with an assessment that considers the simplified definitions.

The definition of TIS can be simplified to:

$$TIS = \frac{P_s \cdot \Delta N_0}{\eta}$$

- Ps = Conducted sensitivity
- η = Antenna efficiency (including cable losses, and so on.)
- ΔNo = Noise floor elevation due to radiated self-jammers (AWGN)

The definition of Total Radiated Power can be simplified to:

$$TRP = P_t \cdot \eta$$

- Pt = Conducted Transmit Power
- η = Antenna efficiency (including cable losses, and so on.)

The conducted sensitivity and conducted transmit power is measured as part of the stand-alone module certification and the values remain valid when considering certification of the host device however if deemed necessary by the operator this test can also be readily repeated in-situ (module installed in the host device) using standardized test equipment.

For large form factor host devices it is expected that antenna(s) are off-module and integrated into the host itself with coaxial cable routed to the embedded module. The host device antenna efficiency can be assessed through test or computational methods including the losses in the cable connections to the module.

If the embedded module is tested and certified using a “reference antenna” and a physically comparable antenna is used in the host device then this may be sufficient for TRP assessment of the host device and for those host devices with inherently “electromagnetically quiet” environments may also satisfy assessment for radiated sensitivity.

For host devices that contain potential sources of electromagnetic noise, this noise contribution (ΔNo) that directly impacts the radiated sensitivity of the host device can be assessed using noise signature methods.

- Spectrum Analyzer Measurement
  - Host located WWAN antenna cable removed from embedded module and connected to spectrum analyzer
    - Measures emissions from host device that couples into WWAN antenna
  - Host device under test isolated in shielded enclosure
    - Measurement cable passes through bulkhead of enclosure
- Embedded Receiver-Based Measurement
  - Noise signature (profiling) capability embedded in module chipset
    - Application runs on either host device processor or cabled (USB) test notebook
  - Accesses WWAN module directly and reports measured power
    - Self-interference is measured by the WWAN module itself
      - Received power (RSSI) monitoring is universal across WWAN receivers
  - Host device under test isolated in shielded enclosure

“Noise profiling” or “Noise Signature” methodology is accepted today by operators in assessing the radiated performance of embedded devices and was recently introduced as an acceptable method for assessing “parent/child” notebooks in the PTCRB certification process.

8 Guidelines for Security and Fraud Risk Management

8.1 Security

The GSM family of technologies is fundamentally secure and embedded services offer an unparalleled level of intrinsic security. However, as with any technology solution there are some risks that require consideration. The following constitutes high level guidelines on the key security issues.

8.1.1 Tampering and theft

It is likely that at some stage of the device lifecycle, an attempt may be made to tamper with or steal the device. Consequently, thought must be given to the physical security design of the device and how it is physically secured in its environment.

The device must have a UICC reader which is directly (electrically) connected to the embedded module.

If the UICC is removed, for whatever reason, then all mobile connections and data sessions (2G, 3G, LTE for example) should be automatically terminated. All temporary key material should be deleted.

8.1.2 Malware

Over the last few years, there has been an increase in malware affecting mobile devices. Most viruses are transmitted over the internet, but they can also be transmitted via Bluetooth and SMS. Controlling Bluetooth connectivity and monitoring traffic on the device should be considered and any unusual usage should be examined and appropriate action taken. A secure channel should be established between applications on the embedded module and applications on the UICC to prevent fraudulent attack or compromise by malware.

8.1.3 Diagnosis and privacy

It is good practice to provide any embedded mobile product with an ability to remotely diagnose issues. Similarly, privacy requirements and concerns of data subjects need to be clearly understood and an ability to report on usage and resolve issues needs to be developed and implemented.

8.1.4 Unique IMEIs

The International Mobile Equipment Identifier (IMEI) uniquely identifies every mobile device. It is mandatory to have a unique and tamper-proof IMEI to comply with 3GPP standards [40] and to help with the identification of devices.

8.1.5 Firmware updates

It is important to consider future requirements and potential security issues. It is recommended that embedded mobile devices should be resilient to emerging threats and technical advances by supporting secure (certified and signed), remote firmware updates.

8.1.6 Credentials

The devices should securely store authentication credentials (for example user name / certificates etc.) and make them available only for authorised applications.

8.2 Data Privacy

EM device and application developers should consider how the collection, storage and transfer of personal data will be performed and secured, given the privacy regimes in different jurisdictions, and what encryption mechanisms are appropriate. Developers should also provide the owners of personal data on EM devices with the ability to wipe their data from the devices.

8.3 Fraud Risk Management Guidelines

EM devices will often be unattended, and therefore are more susceptible to tampering. An attacker may be motivated to tamper with an EM device in order to steal mobile service (for example by removing and using the U(SIM) in another mobile device), or to suppress payment or usage-related messages sent from the EM device (for example utility meter, road tolling system). Unauthorised use of EM devices may also go unnoticed for longer periods of time compared to traditional mobile devices.

Fraud management for EM applications, in common with other mobile services, relies on a combination of business processes and security measures to prevent unauthorised access to networks and systems, and the rapid detection of suspicious activity that could potentially be fraudulent.

The following fraud management recommendations should be observed by the MNO providing connectivity and/or service provider when deploying EM applications to minimise the risk of the U(SIM) from the EM device being used for theft of service:

- Restrict services to the minimum required by the EM application.
- Develop a normal usage profile for predictable EM applications, and
    - Limit traffic volumes to those that might be reasonably required for the application.
    - Monitor usage, generate alarms on high usage or deviations from the normal profile and respond within a relevant timescale
- Where feasible, restrict IMSIs to only work with a specific range of IMEIs.
- Where feasible, securely provision EM applications through the use of IPSec to use dedicated private APN's intended solely for EM services.

The MNO and/or service provider should agree a process and service level agreement (SLA) with its EM customer that describes the obligations and liability of each party if fraud occurs.

To ensure the integrity of the smartcard used in EM applications, and its authentication data, it is essential that the supplier-side manufacturing environment is secure. MNOs are encouraged to source their smart cards from suppliers accredited under the GSMA Security Accreditation Scheme (www.gsma.com/sas).

9 Guidelines for Network Aspects

9.1 3GPP Release 10 deployment guidelines

3GPP Release 10 provides a number of features for overload control, in order to protect the network from excessive signaling from large numbers of devices. The features work whether the device is an embedded mobile device, or not.

The signaling from large numbers of devices is a concern in at least two situations:

- When an application (running in many devices) requests many devices to do "something" at the same time; and/or
- When many devices are roamers and their serving network fails, then they can all move onto the local competing networks, and potentially overload the network(s) which have not (yet) failed.

The main Release 10 features for overload protection cover:

- In GSM, “implicit reject” functionality for devices configured for “low access priority”
- In GSM, UMTS and LTE signaling from the device to the radio access network and to the core network to indicate that the device is configured for “low access priority”. In the LTE and UMTS radio access network specifications, the indicator is named “delay tolerant”.
- Congestion control using Backoff timers and Extended Wait Timer
- Congestion control using Extended Access Barring
- Per device, periodic updating timers.
- Some additional signaling optimizations as described in 3GPP TS 23.060 [50], Release 10 chapter 5.3.13.2.

9.1.1 Guideline

GSMA recommends the implementation of the 3GPP Release 10 overload protection features outlined in this chapter. Specific guidelines for devices, home network, and serving network are described below.

9.2 3GPP Rel-10 Implementation Guidelines for Devices

9.2.1 Support of extended periodic timers

9.2.1.1 Description

3GPP Release 10 introduced per-device timers for Periodic Location Area Update (PLU) and Periodic Routing Area / Tracking Area Update (PRU, PTU). Release 10 also increased the maximum value of these timers.

9.2.1.2 Considerations:

Periodic Updating is a useful feature for devices that move in and out of coverage and might miss a mobile terminating event while out of coverage.

An operator can for instance configure subscriptions for a M2M service provider with stationary smart meters with a longer update timer compared to subscriptions for a M2M service provider within the automotive industry.

A Visited Public Mobile Network (VPMN) can either use the timer configured by the HPMN for a particular device in the roaming scenario, or if this isn't available, use its locally defined timer.

9.2.1.3 Guidelines

It will be necessary for the device to support the extended periodic timers, both for PLU (for circuit switched (CS) domain), PRU/PTU (for packet-switched (PS) domain).

Support for both PLU and PRU is needed, as the device needs to operate in networks which do not support combined CS-PS attach (via the Gs interface from SGSN-MSC).

9.2.2 Interface with USIM

9.2.2.1 Considerations

The overload protection configuration parameters can be stored on a USIM.

9.2.2.2 Guidelines

The device must be able to read a USIM, even if it is a 2G only device.

9.3 3GPP Rel-10 Implementation Guidelines for setting subscription & device parameters by the home MNO

Correct operation of the 3GPP Release 10 congestion control mechanisms in the visited network relies on optimal configuration of the device and/or subscription parameters by the home network.

Without widespread adoption of the settings across the operator community, the protection mechanisms will not work effectively. Specifically, incoming visitors will not have suitable settings and local competitors of the hosting network will be unable to protect themselves.

9.3.1 Device Parameters set by the home network

This section describes the six configuration parameters defined for the device. It provides a description of each parameter, describes the possible values of the parameter, considerations to be taken when setting the parameter value, and associated implementation guidelines.

In some cases, the expected behaviour of the application, or the revenue value of the traffic, need to be considered when setting the parameter value. Section 9.3.3 gives examples of how the parameters could be set for some M2M verticals.

There are several means to configure these parameters:

- **OMA DM**: to re-configure the terminal's NAS configuration Management Object (MO), see 3GPP TS 24.368 [51]
- **SIM OTA**: to configure the USIM's file EFNASCONFIG (Non Access Stratum Configuration), see 3GPP TS 31.102 [11].
- The terminal can also be configured using device-specific method (e.g. at production time)

Note that if both USIM and OMA DM values are present, 3GPP have specified that the USIM values take precedence (see TS 22.368 [52] section 7.1.1, and TS 31.102 [11] section 4.2.94).

9.3.1.1 Allocation of Low Access Priority (LAP) to subscribers

Description

3GPP Release 10 introduces the concept Low Access Priority indicator. The operator can set the LAP indicator in “low priority” devices, where the application(s) can tolerate longer access delays. The LAP indicator can be used by the network to reject such a device from access, and assign a back-off timer preventing the device from immediately repeating the access attempt. The mechanism is primarily intended to combat high network load in radio access network and core network nodes.

Possible Values

The parameter can either have the value 1 (low priority) or not be present at all.

Considerations

A well suited allocation of LAP to subscriptions is critical to make overload protection work. For example 3GPP Release 10 congestion control via back-off timers in the visited radio access network is only applied to LAP subscribers.

In Release 10, the Low Access Priority indicator is a device property, meaning that communication from all applications on the device (except emergency-related and the special SIM access classes 11-15) is considered as low priority.

Guideline

In general, the home operator should provision the LAP indicator for embedded mobile subscriptions which are susceptible to cause network overload. The LAP indicator should be provisioned even for subscriptions that are permanently or mostly roaming, in order to protect the visited network.

As described by TS 23.060 [50], the setting for LAP shall be identical to the setting for Extended Access Barring for applicable embedded mobile devices.

9.3.1.2 Extended access barring

Description

Under certain circumstances, it is desirable to prevent mobile devices from making access attempts or responding to pages in specified areas of a mobile network (so called Access Barring). It is possible for the mobile to decode if it is barred or not with the help of broadcasted information. Extended Access Barring (EAB) is an additional access barring feature introduced in GERAN for Release 10 which makes it possible for the operator to either only bar roaming devices, or to only bar roaming devices not on the most preferred network in that country.

Possible Values

1= EAB is applied for the device

0= EAB does not apply for the device

Guideline

The home operator shall only apply EAB for those devices which have LAP applied, and shall not apply EAB for those devices which do not have LAP applied.

9.3.1.3 Minimum periodic search timer

Description

Before Release 10, roaming mobiles do a background search for “more preferred” mobile networks in that country using the timer EF_{HPPLMN} (Higher Priority PLMN search period) typically set to 6 or 12 minutes.

Consequentially if the most preferred network fails, masses of devices would move to a non-preferred network in that country, do location area and routeing area updates on that network, and every 6 or 12 minutes attempt (and fail) to return to the preferred network.

The “minimum periodic search timer” is intended to reduce the frequency of this behaviour.

The device uses the larger of the “minimum periodic search timer” and the value in EF_{HPPLMN}, to control is background search for more preferred networks.

Possible Values:

The parameter can be in the range 0-255 minutes.

Considerations

If the timer is set too short, the preferred network may not have recovered. If it is set too long, a lot of traffic may have been carried by networks other than the preferred network.

Guideline

For low revenue devices, recommendation is to use a high value, 255 minutes. For high revenue devices, recommend to use a lower value, 20 minutes.

9.3.1.4 Control of ‘Network Mode of Operation I’ behaviour

Description

NMO-I (Network Mode of Operation I) enables a device to perform combined attach towards the packet switched domain. Otherwise, the device will perform individual attaches to the circuit switched and packet switched domains.

The use of combined attach reduces the signalling load on the serving network. However, this might not be beneficial for the operator to apply for all categories of devices.

Extended NMO-I is introduced in Release 10 to allow the operator to control if a device should perform combined attach, or not. The serving network must broadcast that it supports “extended NMO-I” for this feature to work.

Possible Values

1=NMO-I indication is used, if available;

0=NMO-I is not used

Considerations

A VPMN can choose whether or not to use “long PLU and long PRU” timers, or whether or not to use “long PRU timer and extended NMO-I”. It is therefore important that the HPMN configures the device to be able to use extended NMO-I, unless there is some compelling service requirement to not do so.

Guideline

It is recommended that all data centric devices are configured 'NMO-I indication is used, if available'.

9.3.1.5 Attach with IMSI indicator

Description

If set, then when registering with a new mobile network, the device will present its IMSI rather than a temporary identify. This reduces the signalling load on the new network, as it doesn't have to try and resolve the temporary id and subsequently request the IMSI from the device. This will help a recipient network if it has to manage an incoming 'avalanche' of device registrations coming from a failed network.

Possible values:

1=attach with IMSI performed when moving to non-equivalent PLMN;

0=normal behaviour

Considerations:

The disadvantage of setting this parameter is that if the device moves between networks and attaches using the IMSI, then any active PDP context will be torn down. This would also be the case if the device presented an unresolvable TMSI to the new network.

Note that if the device is moving between equivalent mobile networks (based on the Release 99 equivalent feature) then Attach with IMSI is not invoked.

Guideline

This parameter should be set to 1 for all embedded mobile devices, unless the home MNO has national roaming agreements which allow the use of the previous network's TMSI without using equivalent functionality.

It should always be set to 1 for stationary devices, even if national roaming is in place.

9.3.1.6 Timer T3245 behaviour

Description

This parameter controls whether timer T3245 is used by the device. If T3245 is used, then on expiry it causes the device to erase the forbidden network list and to remove any "invalid SIM" setting. The value of T3245 is defined in 3GPP TS 24.008 [53], and is randomly chosen by the device from the range 24 to 48 hours.

Possible Values

1=T3245 used

0=T3245 not used

Considerations

If T3245 is not used, then the device needs to be power-cycled to remove the "invalid SIM" setting and successful 'manual network reselection' is needed to remove entries from the forbidden PLMN list itself. This requires manual intervention (e.g. a site visit to every electricity meter), or, discourages application developers to automatically power cycle the device when a reject message is received (which causes other kinds of problems)

The T3245 timer should be used by embedded mobile devices which are not easy to service. For example, if a smart meter receives a fatal error such as "IMSI unknown" it will add the network to the forbidden list and never connect to it. It is expensive to send a service technician to the smart meter to power cycle it. Therefore, the T3245 expiry acts as an automated mechanism to flush the forbidden network list, thereby enabling the smart meter to function again.

Guideline

This timer is recommended to be used for devices which are intended to run without human intervention.

9.3.2 Subscription parameters to be transferred to the visited MNO

It is necessary that, where possible, the HPMN sets the PRU/PTU and PLU values for M2M devices to large values. This protects other mobile networks in the country of the VPMN in case the VPMN fails. Use of large values is useful because this slows down the rate at which devices detect the failure of the VPMN, giving more time for the VPMN to be returned to service.

9.3.2.1 PLU timer value per subscriber

Description

This is a subscription parameter set in the Home Subscriber Server (HSS) and stored in the VPMN, to set the Periodic Location Updating value for the CS domain.

Possible Values

0 – 4294967295 seconds.

Considerations

A relatively short PLU timer value is needed for applications which have a need for immediacy with mobile terminating communications, i.e. there is a need to contact the device as soon as possible once it comes back into coverage. The downside of using a large PLU timer is that if the nature of the device is that it can be expected to regularly move in and out of network coverage (for example a track & trace device), then the application may take longer to become aware of an attempted mobile terminating communication.

Guideline

Recommend typical value of PLU for embedded mobile devices to be 24 hours, unless the nature of the application calls for immediacy of mobile terminating CS domain (voice and/or SMS) communications.

9.3.2.2 PRU/PTU timer value per subscriber

Description

This is a subscription parameter set in HSS and stored in the VPMN, to set the Periodic Routing Update value for the PS domain. It works on the same basis as the PLU timer described above.

Possible values

0 – 4294967295 seconds

Considerations

None

Guideline

Recommend typical value of PRU for embedded mobile devices to be 24 hours, unless the nature of the application calls for immediacy of PS domain mobile terminating communications.

9.3.3 Example settings for M2M verticals

9.3.3.1 Low mobility, low revenue (e.g. a Smart meter)

Parameter	Value	Meaning
LAP	1	Set
EAB	1	Set
Min periodic search timer	255 minutes	-
NMO-I	1	Set
Attach with IMSI	1	Yes
T3245	1	Used

Table 10: Low mobility, low revenue

9.3.3.2 High mobility, high revenue (e.g. Automotive with infoservices)

Parameter	Value	Meaning
LAP	not present	-
EAB	0	Not set
Min periodic search timer	20 minutes	-
NMO-I	1	Set
Attach with IMSI	1	Yes
T3245	1	Used

Table 11: High mobility, high revenue

9.4 3GPP Rel-10 Implementation guidelines for networks serving the device

Without prior preparation, with large numbers of roaming devices, failure of one mobile network might have a domino effect on the other local competing networks, potentially leading to failure of all the networks.

9.4.1 Long PRU/PTU timer – default value in SGSN

The PRU (periodic routing update) / PTU (periodic tracking update) timer is used in the Packet Switched domain.

9.4.1.1 Guideline

If the mobile supports a long PRU/PTU, and the SGSN does not receive a timer value from the HLR/HSS, then the SGSN should allocate default value to a device configured for LAP.

Recommended value: 12 hours.

9.4.2 Extended NMO-I or Long PLU

9.4.2.1 Guidelines

The visited network should support either a long PLU timer, or the extended NMO-I feature to manage M2M devices with a circuit switched service (e.g. SMS).

It is recommended that the VPMN supports the extended NMO-I feature, meaning that combined packet-switched and circuit-switched attach is supported, using the Gs interface.

If extended NMO-I is deployed, then its use must be broadcast continually (i.e. don't wait for overload situation), and it must be broadcast on all cells within a location area.

Changing the NMO will cause all mobile devices in that area to immediately perform updates to the network.

If the VPMN chooses not to implement extended NMO-I (for example, if Gs isn’t supported) then the VPMN should implement a long default PLU timer for Low Access Priority devices.

9.4.3 Reject causes with back-off timer: for core network

9.4.3.1 Description

When performing mobility management procedures (e.g. location update or routing area update), or session management procedures (e.g. PDP context activation) the serving core network can send a back-off timer to the requesting device - "don't retry for time x". Two different types of control of the back-off timer are available:

- General mobility management control. The network may reject messages including the “low access priority indicator” before rejecting messages without the “low access priority indicator”.
- APN based congestion control. The network may reject requests from UEs to a certain APN. This can help the operator to control applications using a specific APN.

9.4.3.2 Guideline

Serving networks should consider using:

- The general mobility management control for the devices with LAP indicator.
- APN based congestion control for the APNs as a means to identify embedded mobile devices, if a dedicated APN is used for such devices.

9.4.4 Reject causes with back-off timer: for Radio Resource

9.4.4.1 Description

3GPP Release 10 provides the ability for the radio access network to reject a request with a longer back-off timer than was defined previously, also called Extended Wait Timer.

9.4.4.2 Possible values

UTRA/EUTRA:	time = 1..1800s (was previously 16 seconds)
GERAN:	time = 0..255 s

The radio access network will only use the extended wait timer if the device had signalled LAP in its access request, see 3GPP TS 23.060 section 5.3.13.3.

9.4.4.3 Guideline

The visited network must decide the back-off timer values to apply. Networks are recommended to spread the values given to the back-off timer over a range, to avoid the same access problem occurring at a predictable time in the future.

9.4.5 Implicit Reject in GSM Radio Network

This Release 10 feature is a powerful tool which the GSM base transceiver station (BTS) in the serving network can use to dynamically and quickly control the (over)load from Low Access Priority devices on its RACH, AGCH and SDCCH channels.

Before requesting a signalling channel, a device that has LAP assigned will check the ‘Paging’ and ‘Access Grant’ broadcast channels for 20ms. If the BTS has set the ‘implicit reject’ flag (one flag for circuit switched and one flag for packet switched) then the mobile will not request a signalling channel, but will back off for a locally generated random period.

9.4.5.1 Guideline

The visited network should procure the ‘Implicit Reject’ functionality.

9.5 Implementation guidelines for device application designers

9.5.1 Data aggregation within terminals

All communication over cellular systems triggers events which generates signalling between network entities. Sending a small or large chunk of data generates the same amount of signalling. Thus to keep the signalling load on the network low, it is better to send larger chunks of data less frequently compared to small chunks frequent.

9.5.1.1 Guideline

Reduce the number of connections between the terminal and network by collecting data in lager chunks before sending. If several applications reside on the same terminal, coordinate the application’s network communication.

Within each connection, send data in as concentrated a manner as possible since even small time separations of a few seconds may (depending on network settings) generate unnecessary network signalling load.

9.5.2 Avoid synchronized network access between terminals

To avoid signalling and user data traffic peaks in the network, communication with different terminals should not be synchronized in time. Preferably, non time critical communication should be deferred to off network load peak time.

Examples of synchronized communications are provided below

- Automotive - periodic reporting of diagnostic information on a daily / weekly basis. If the same client is present in a large number of vehicles from a manufacturer, the client should ensure that reporting at a specific time but is randomised within a time window.
- Energy - *r*eporting of a change in energy generation. If the same client is present in a large number of homes within a city region, and the client detects a change of energy generation due to a change in local weather, then the client should be aware that this event is shared by possibly many other clients in the region – so avoid the risk of synchronised reporting to the server by introducing a randomising element.
- Energy - reporting of a power failure by a smart meter. This is likely to be highly synchronised and (for the PLMN operator) unexpected. (The GSM base station’s

Implicit Reject function is useful in this case – provided that the smart meters have been configured to use Low Access Priority).

9.5.2.1 Guideline

To avoid synchronization effects, communication with different terminals should be spread out in time over off-peak traffic hours. This applies both for terminal and server initiated communication. A means to do this is to randomize communication in time.

9.6 Network Management and Optimisation

9.6.1 High Level Requirement

As embedded devices connect to the network, they will occupy network resources - both RF elements (channel, power, codes, etc.) and Core Network elements (backhaul, IP addressing, etc.).

These new connected devices and associated applications have a need for network connectivity that may be intermittent and sometimes scheduled. Any service request denials from the network, due to lack of availability of the above stated network resources, could have severe consequences on the operation of these embedded devices within vertical market segments such as automotive and healthcare.

9.6.2 Guidelines

Since the needs of the embedded devices for network resources are more ad hoc than mobile devices, mobile network operators (MNOs) should develop some network monitoring tools and diagnostics capability to plan their networks efficiently. Also, MNOs should pro-actively manage their resource utilization to avoid denying any service requests from the ad hoc embedded devices:

- Develop network monitoring capabilities for embedded modules
- Develop guidelines for activation, provisioning and registering of modules for efficient network planning
- Develop network management tools for optimal network capacity management

9.7 Signalling Traffic from Non-Activated or Out-of-Subscription SIMs

9.7.1 High Level Requirement

As the number of EM devices and traffic from these devices increase, it must be possible to stop unexpected signalling effectively monitor network quality and detect authentication problems.

9.7.2 Considerations

There are several use cases that might lead to the potentially disruptive high volumes of signalling traffic. These include non-activated SIMs, expired SIMs or SIMs temporarily out of subscription:

- Non-activated SIMs: Increasingly, embedded device manufacturers (for example, car manufacturers) fit a SIM by default to every device (for example, in-vehicle systems (IVS)). This SIM card is not activated in any networks' HLR until the owner of the device subscribes to an EM-related service (which they can do at any time, or never).

- Expired SIMs or SIMs temporarily out of subscription: new EM devices are sometimes sold to end-users bundled with free EM-enabled service for a year (for example, navigation service in a car), which is not renewed upon its expiration. Similarly, EM-enabled services might be stopped temporarily with a view to be renewed at a later date; as a result, the EM SIM will be temporarily out of subscription.

This behaviour has been observed with the cars of at least one specific car manufacturer, where embedded SIM cards are periodically attempting to authenticate to a network; if the SIM is not activated or out of subscription, the authentication fails. Although the number of SIM authentication attempts is not significantly high today compared with all other attempts, the number of authentication failures is significant. For example, in the specific case observed between two roaming partners, the normal 1% authentication failure rate has increased to anything up to 60%. This means that it is very difficult to detect real authentication problems, thus impacting roaming quality monitoring.

9.7.3 Guideline

It is not recommended that the EM device signalling capability is stopped altogether, for example, when the connectivity is turned off completely via an instruction from the network, as this would introduce a significant new denial-of-service security risk,

It is recommended that some limitations are imposed on the frequency of signalling either via embedded devices or network-based modifications.

One to reduce the volume of signalling traffic would be to use the T3245 timer (see section 9.3.1.6). For example, the network could configure the device to use the T3245 timer, then send it a forbidden PLMN error message (e.g. IMSI unknown in HLR), which will cause the device to not retry for 24 to 48 hours, after which it will automatically clear it’s forbidden PLMN list and retry.

It might also be possible to modify the provisioning process for the EM SIM activation. More specific guidelines may be identified once the Embedded SIM TF output becomes available.

9.8 Numbering Resources

9.8.1 High Level Requirement

The anticipated growth of embedded devices is expected to increase the demand for E.164 [54] MSISDN resources. A large number of EM services are deployed using circuit switched architecture, even where a traditional “dialable” number may not be required. This might lead to the shortage of the numbering resources for new Machine Type Communications (MTC) services. Providing for the expected future growth means ensuring that alternatives to public numbering resources need to be considered as addresses.

9.8.2 Considerations

Numbering resources are already in short supply in some markets, for example, in the US and a number of European markets [56]. To address this issue, in the short term, geographic numbers are likely to be migrated to 12+ digit numbers by 2020 and incur significant costs. Where EM services require no human interaction, alternatives to the existing public numbering schemes need to be considered. Work on the development of such alternatives currently takes place in such standards bodies as ETSI, 3GPP and ITU.

At 3GPP SA1, different alternative solutions for short, midterm and long term are proposed in the Study on Alternatives to E.164 for Machine-Type Communications. These solutions are subject to 3GPP technical specification group modifications and approval.

An interim midterm solution for number shortage is to extend the number of digits in the E.164 number on dedicated ranges that are currently spare and not yet assigned.

The suggested long term solution for E.164 number shortage for M2M is to use IPV6 addressing with corresponding identifiers (for example SIP addresses URIs/URLs) and remove the reliance on MSISDNs. This solution requires an evolved packet core network and may need an upgrade of mobile operators' networks. This long term solution will need actions in 3GPP standards.

While planning the migration to IPv6, the issues that need to be considered include the strategy for the development of EM applications, impact on the infrastructure, operational costs and security.

9.8.3 Guideline

It is recommended that industry wide solution is developed for the numbering problem to avoid the implementation of costly interim single-market solutions.

9.9 Network Selection Guideline

Different network types with different characteristics (e.g. GSM, WCDMA, LTE, WLAN) may be available to a mobile network operator. Mobile network operators should consider distributing different types of EM traffic across their different networks based on the capabilities of the network, the characteristics of the traffic and the requirements of the application. This should be done to satisfy end-user quality requirements and to protect the MNO's network from signalling congestion and overload.

EM device and application developers should consider the appropriate access network to be used when designing applications. The choice of network to be requested by an EM device or application should also consider whether the device is roaming or not in order to avoid any negative effect on the visited network.

9.10 Future Requirements

9.10.1 Device application Requirement – Managing Multi-Application EM Devices

It will certainly occur that a single device, with a single subscription, will need to be used for low priority transmissions and normal/high priority transmissions. e.g. automotive (diagnostics = LAP, eCall = not LAP); burglar alarm (heartbeat = LAP; move PLMN = LAP; alarm = not LAP).

3GPP Release 10 standards do not address the need for a single device, with multiple resident applications, to generate both LAP communications and non-LAP communications. 3GPP is working on supporting this for Release 11.

9.10.2 HSS/HLR Overload Control

The 3GPP Release 10 LAP and EAB mechanisms (described in section 9.3) can be used to resolve overload or congestion in the radio access network and the core network. However, scenarios may arise in which the HSS/HLR may be suffering from overload or congestion when the core and radio access networks are not. Enhancements to the 3GPP standards may be required to define HSS/HLR specific overload control mechanisms in such scenarios where the EAB/LAP based congestion control mechanisms may not be effective.

9.10.3 Support for Indication of Subscriber Types and Services/Applications

In addition to implementing access network enhancements to support the anticipated growth of EM traffic, enhancements should also be considered for protecting the core network. To efficiently use network resources and prevent core network overload, dynamic policy control and charging (PCC) should be considered for use in managing the network, and scheduling and routing traffic according to network congestion status, subscriber and service /application types, user rate plans etc.

To allow the network to be subscriber and services aware, a mechanism would be required to provide the interaction between network control and applications and devices. Indications of subscriber types and services/applications will give the subscriber or the application provider the option of easily selecting how the network should treat different applications or application classes for a specific subscriber. It will also give the network the means to handle the traffic priorities accordingly. The subscriber type and service/ application information could also be used for billing, reporting etc., subject to net neutrality considerations in some regions depending on regulatory requirements.

9.10.4 Roaming Transparency for EM Devices

The GSMA Billing, Accounting and Roaming Group (BARG) is working to define principles and a mechanism for facilitating visibility of EM traffic in a roaming scenario.

10 Guidelines for Roaming

Seamless roaming will be a success factor for EM in the same manner that it has been for GSM. Depending on the application, roaming may be required occasionally, persistently or permanently, as described below. Even static EM devices such as utility meters may require roaming capability.

For some applications, most service will be required within the home network, and roaming will only be required occasionally. For example:

- Private car equipped with M2M-enabled navigation, breakdown support and infotainment services travelling across national borders for holidays a few times per year.
- Cardiac monitor worn by patient who takes occasional foreign trips.

Many EM devices may be permanently or persistently deployed in a roaming environment. For example:

- A telematics service provider may deploy (U)SIM cards from a single operator into trucks that are sold internationally by the truck manufacturer. A truck may never visit the home network of the installed (U)SIM card during its lifetime.
- A multinational energy provider may install smart meters in several countries using (U)SIM cards from a single operator in order to minimise the number of parties it has to deal with to manage connectivity.
- A mobile network operator that is contracted to provide connectivity for smart utility meters may provide its customer with roaming (U)SIM cards from a foreign mobile network operator partner (for example within the same corporate operator group) to take advantage of the coverage of its national competitors in areas where it has no coverage.

Widespread and permanent international deployment of EM devices potentially containing a subscription from a single operator will change the support demands on visited networks hosting large numbers of these devices. Adaptations in the following areas of roaming network resource and efficiency management should be considered

10.1 Efficient Use of Roaming Resources

Very large scale deployments of EM devices will require mobile network operators to review their network configurations to ensure good service both to traditional users and to EM devices within the network resources available. This will be especially relevant in a roaming context, where unnecessary and inefficient signalling between the home networks of large numbers of EM devices and the visited network could cause congestion on signalling links and negatively impact roaming service quality. The impact of large numbers of roaming EM devices may also place a capacity and/or processing burden on roaming network infrastructure such as the Visited Location Register (VLR).

Roaming security and fraud protection should not be sacrificed when optimising signalling. For example, reducing the authentication frequency of inbound roaming devices is not recommended.

10.2 Roaming Congestion Control & Overload

In general, the ability for mobile devices to attach to any available network when roaming creates challenges for networks in the visited country when there are very large numbers of EM devices persistently or permanently roaming. Section 9 describes risks and recommendation countermeasures associated with congestion and overload. The following specific risk associated with roaming is worth highlighting:

- An external event may trigger massive numbers of roaming EM devices to attach/connect all at once. For example, an earthquake or power cut causes simultaneous reporting by burglar alarms, or a fault in a visited network triggers massive numbers of roaming EM devices to switch to another visited network within a short period.

The network aspects guidelines in section 9 should be followed to ensure that roaming services can continue to be delivered effectively and efficiently to all customers in an environment involving large numbers of EM devices.

11 Service Quality and Availability

Mobile networks can provide a connectivity solution that is more than adequate for the majority of EM applications. These applications will deliver significant benefits that are not possible via existing services. For example:

- Remote health monitoring solutions will alleviate the need for patients to physically attend a clinic for check-ups; instead, readings can be taken remotely and relayed using an EM device over the mobile network to the patient’s doctor. Even if a patient is temporarily out of mobile coverage, data can be stored in the device and sent once coverage is regained. Overall, the EM solution provides a much more comprehensive picture of the patient’s health than is currently possible without remote monitoring.
- EM-enabled automotive emergency and breakdown assistance will provide significant advantages compared to existing solutions, due in particular to the automated establishment of communications in an emergency and the transmission of exact location to responders. In rare cases, vehicles may be in area outside the coverage of mobile networks. However, the vast majority of support requests take place in areas with extensive network coverage so the benefits of this initiative are enormous.

To maximise the availability of the benefits possible from EM solutions, those that are used for critical applications should monitor and alert the user of connectivity status, and implement application-level mechanisms to maintain the best possible level of service in the event of radio resource scarcity. EM devices associated with such applications should be capable of providing a minimal level of diagnostics and control (via SMS, for example) in such a scenario. EM application servers also need tolerance and intelligence mechanisms in order to maintain the best possible level of service in the absence of a guaranteed connection with EM client devices.

12 Specific Guidelines for Key Vertical Sectors

The chapter is structured in several sections:

- Automotive
- Consumer electronics, including education
- m-Health
- Smart metering

Each section has the following format:

- Ecosystem description
- Representative use cases
- Embedded module requirements and solution design implications

12.1 Automotive

The focus of this section is on the development of automotive guidelines for telematics and infotainment services that will be common across the automotive industry and will be equally applicable for the most part across all automotive OEMs, independent of region.

For the purpose of this document, automotive telematics and infotainment refers to the use of telecommunications devices to send, receive and store information within automobiles and may also include the processing of such information.

12.1.1 Ecosystem Description

The key players in the EM automotive segment ecosystem are as follows:

- Auto manufacturers (including their dealerships)
- Automotive suppliers
- Chipset manufacturers
- Consumers/motorists
- Enterprises
- Embedded module manufacturers
- Mobile network operator
- Smartcard (UICC) manufacturers
- Standards/specifications setting organizations
- Third-party service provider (including application developers)

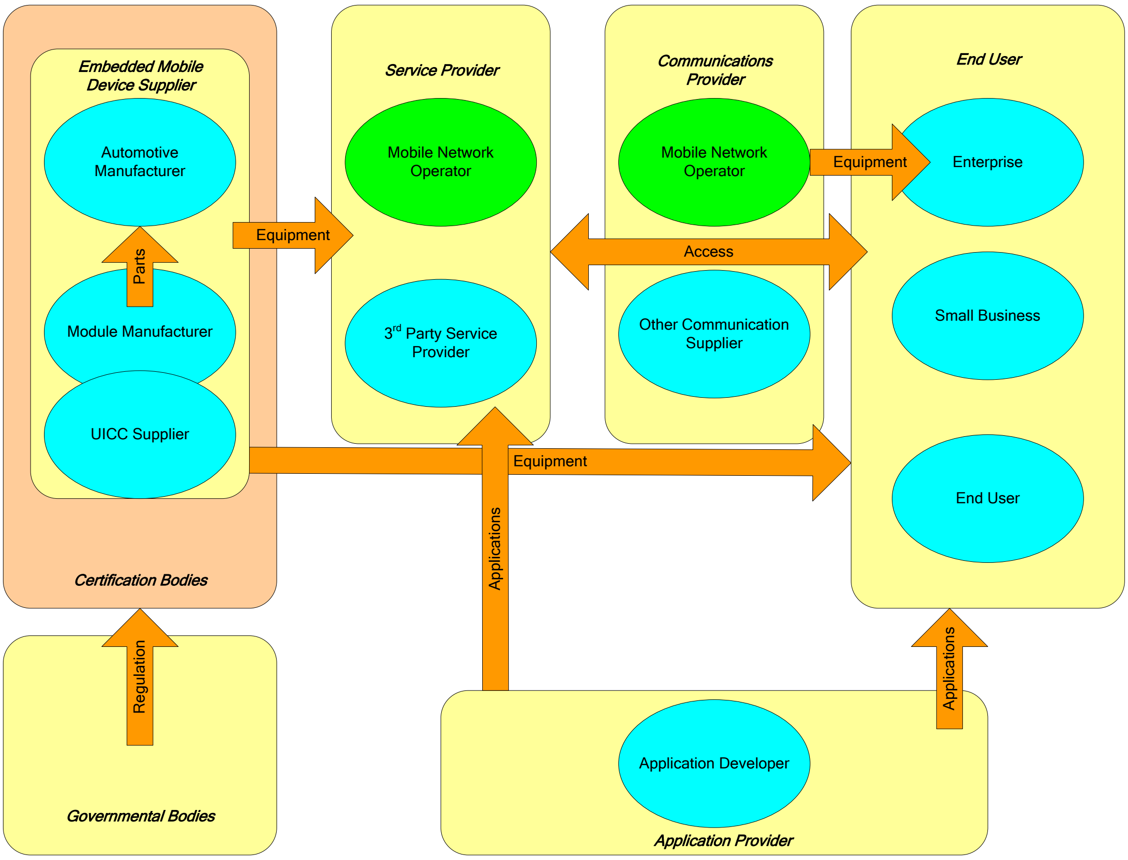


Figure 10: Automotive Embedded Mobile Eco-System

12.1.1.1 End Users

End User/Owner/Enterprise (the Customer)

This is the user of the services/applications being provided in the automobile and may include the owner of the vehicle, or authorized user of the vehicle to which the services or applications are being delivered.

12.1.1.2 Embedded Device Supply Chain

Automotive Manufacturer

Directly or indirectly, the supplier of the vehicle to the customer/motorist and integrator of the embedded module; may have an established relationship with the service provider(s).

Auto supplier

Supplier of additional automotive components that might be used in specific use cases, for example, audio, video and gaming connected devices for entertainment services

Embedded Module Manufacturer

The embedded module manufacturer is responsible for the design, development and production of the embedded module. Companies such as these work with the automotive manufacturer to integrate the embedded module into the vehicle.

Smartcard Manufacturer

The entity responsible for the manufacture of the UICC card works with the MNO to ensure compatibility with the mobile network and also with the embedded module vendor to ensure compatibility with the module.

12.1.1.3 Communications and Service Providers

Mobile Network Operator (MNO)

The MNO provides communication network access to the motorist or enterprise owning the automobile. The MNO is the owner of the UICC issued to the customer. In a number of instances, the MNO may also be the service provider.

Third Party Service Provider

This is an entity other than the MNO that will provide a service directly to the customer through use of the embedded module and the issued UICC.

Application Service Provider

The application service provider is the developer and provider of the applications used by the service providers to deliver a specific service.

12.1.1.4 Standards Bodies and Regulators

The standards bodies are responsible for the development of the necessary technical specifications for the embedded modules, smartcards, and the embedded device as required.

12.1.1.5 Certification/Approval Bodies

These are the entities that will undertake the necessary technical testing and subsequent approval of the embedded modules, smartcards, and the embedded device as required.

12.1.2 Representative Embedded Module Services in the Automotive Sector

The following is a short list of high-level services to be supported by the embedded modules:

12.1.2.1 Breakdown Services (bCall)

bCall (breakdown call) services send the current vehicle position to a roadside assistance organization and initiate a voice call. The bCall trigger is usually a switch, which must be pushed by the user in order to activate the service.

An ‘enhanced’ bCall service is where current vehicle diagnostic information is also transmitted, in addition to the vehicle position. This could, in principle, allow the fault to be diagnosed remotely and appropriate action taken.

12.1.2.2 Stolen Vehicle Tracking

The purpose of a Stolen Vehicle Tracking (SVT) system is to facilitate the recovery of the vehicle after theft. Usually, the owner must first report the theft to the police (obtaining a crime report number) prior to contacting their SVT service provider who can obtain (at minimum) the location information but also enable immobilization or speed degradation by remote command.

12.1.2.3 Remote Diagnostics

Remote diagnostic services can broadly be grouped into the following different implementations:

Maintenance minder – when the vehicle reaches a certain mileage the control unit will send a message advising them that the vehicle is due for servicing

Health check – either on a periodic basis, or triggered by a request from the owner, the control unit compiles the vehicle's general status, using inbuilt diagnostic reporting functions, and transmits a diagnostic report

Fault triggered – when a fault is detected with one of the vehicle systems, this triggers the car to send the code and any context information (for example snapshot data)

12.1.2.4 Insurance Services (PAYD)

Pay-As-You-Drive (PAYD) schemes offer insurers the chance to reduce costs, more accurately reflect actual risk and provide more competitive products to the end-user based on getting feedback from the vehicle as to when, where, how or how far the vehicle is being driven.

12.1.2.5 Pan-European eCall

Pan-European eCall is a European Commission specified mandatory (in Europe) emergency service for the automotive vertical sector. These emergency calls are triggered automatically via activation of in-vehicle sensors when an accident occurs (in addition to facilitating manually triggered calls). The in-vehicle eCall directly establishes an emergency voice connection with the relevant Public Service Answering Point, and sends crucial information such as time and location of the accident, and a description of the vehicle involved. The information sent may also include a link to a potential service provider. If the user has subscribed to a service provider, additional information can be sent by the service provider. An alternative, third-party eCall compliant service is also being offered by some automakers.

12.1.2.6 Connected navigation

- *Traffic Reports:* The purpose of a traffic report service is to inform the driver of traffic conditions relevant to the area in which they are driving, or a location on their intended route, so that they may alter their route to avoid heavy traffic if necessary
- *Route Planning (Send-to-car):* The purpose of this service is to provide the user with a means of planning their forthcoming journey using a PC, and to download the chosen destination to the vehicle.
- *Visually-enhanced navigation:* This service provides the user navigation directions that are visually enhanced with real-world video or digital images of the route. Tags or arrows can be superimposed on the video or images to make it clear to the motorist where, and in which direction, turns are to be made.
- *Augmented reality Points of Interest:* Augmented reality technology uses virtual computer-generated imagery to augment elements of a live - direct or indirect - view of the physical real-world environment. Using this technology, point of interest information can be directly superimposed onto a view of the real-world surroundings displayed on either a dashboard LCD screen or projected as a Heads-Up Display on the windshield.

12.1.2.7 Infotainment

- *Information Provisioning:* The purpose of this service is to provide information to driver and passengers, and may include:
    - Mobile TV
    - Internet connectivity for web browsing and email
    - Location-based interactive e-commerce (for example, shopping or restaurant recommendations, user can reserve a table or book cinema tickets)
- *Voice-activated digital concierge services:* The service allows the driver to use natural language to make requests from an automated digital concierge server and obtain rich multimedia responses. The in–vehicle system makes a recording of the driver's speech and transmits this error-free to a voice recognition server over a high-speed packet data connection.

12.1.2.8 Travel and Traffic Assistance

- *Assisted Traffic Regulation:* Certain aspects of traffic regulation measures can be assisted by transmission of static or dynamic non-critical road regulation information to the car. Examples of this service include the transmission and notification about closed roads, dangerous road conditions, highway tolls, speed limits, based on location information, or even a wrong way warning when on one-way roads.
- *Access Control / Parking Zone Management*: Communication and a service infrastructure, combined with stored user or car credentials, could be used to manage access to specific areas, for example; company or private grounds. A gate could be opened by transmitting SIM or other stored credentials, or by typing a PIN on a keypad in the car.
- *Eco-drive:* An eco-driving telematics service enables the recording and transmission of relevant vehicle data. Analysis of this data can generate driver-specific tips to improve vehicle fuel economy, for example by adopting a more fuel-efficient driving style.

12.1.2.9 Cloud Computing for Automotive Embedded Modules

Cloud computing services enable processor and information resources in the network to be shared between many devices. In the case of automotive embedded modules, cloud computing provides a number of benefits: new applications can be deployed on network servers without requiring costly upgrades to the embedded modules, and performing computation and storing information in the network instead of in the embedded modules enables the use of lower-cost modules. For cloud computing to be practical in the context of automotive modules, there must be a high-bandwidth, low-latency connection between the modules and the network servers, so that the applications can quickly respond to user input and provide the results of network computations.

12.1.2.10 Electric Vehicle (EV) Communications

Electric Vehicle (EV) charging is a key application of the Smart Grid. An embedded communications module in the EV connects the EV to the charging infrastructure. The embedded module enables the EV to locate and reserve a charging station near its current location when its battery level is low, and the user can remotely check the charging status of their EV while it is charging. The WAN connection provided by the embedded module supports authentication and billing, and makes it possible for the EV to be commanded to provide power back to the grid during peak usage periods.

12.1.3 Connectivity Use Cases in the Automotive Sector

The use cases for automotive connectivity embrace a variety of situations, with primary distinctions being made according to who pays the connectivity contract and the frequency of modifications to the connectivity use case. The primary automaker use cases, as discussed in the Connected Car Forum, are presented below:

		Use Case Characteristics		
Process	**Connectivity Use Case**	**Description**	**Owner of Connectivity Contract**	**Expected Frequency of Use Case**
Vehicle testing	Test and development of telematics services	Allows automaker to easily test different SIMs in the same car and the same telematics control unit (TCU)	All possibilities	Varied
Vehicle delivery	Initial vehicle production where automaker pays for telematics	SIM is provisioned to the mobile operator according to the vehicle destination	Automaker service contract	Once
Service activation: consumer	Vehicle sale where services are paid by vehicle owner	SIM is provisioned to the customer's mobile operator when the vehicle is sold	Customer contract	Once
Connected Car Service Operation:				
Automaker connectivity contractual changes: Small scale	Vehicle moves permanently to new region where automaker pays for telematics	Automaker can provision SIM to their local mobile operator	Automaker service contract	Infrequent
Automaker connectivity contractual changes: Frequent	In order to maximise performance characteristics (i.e. signal strength, cost, application package, etc.), connectivity is switched across operators domestically. Example. Car is within country A and is switching MNOs according to defined parameters (e.g. signal strength, cost, application package).	Automaker can provision SIM to their local mobile operator	Automaker service contract	Every second/ minute
	Traveller roaming: Car is travelling temporarily from country A to country B. Subscription is changed from	Automaker can provision SIM to their local	Automaker service contract	Every hour/day/ week

Process	Connectivity Use Case	Use Case Characteristics		
		Description	Owner of Connectivity Contract	Expected Frequency of Use Case
	local MNO in country A to local MNO in country B	mobile operator		
Customer Service Changes	Vehicle owner changes MNO (where owner pays for telematics services)	Customer can provision SIM to their new mobile operator	Customer contract/ automaker service contract	Every 1-2 year
	Car is sold to a new owner (where owner pays for telematics services)	New owner can provision SIM to their mobile operator	Customer Contract/ automaker service contract	Every 3-4 year
	Car is driven by a new driver (where owner pays for telematics services); This use case is particularly interesting for car-sharing programmes.	New driver can provision SIM to their mobile operator	Customer contract/ automaker service contract	Every hour/day/ week
Service cancellation	Service subscription is stopped	Automaker or customer can cancel subscription	All possibilities	Infrequent
Hardware changes	Operational problem: Telematics control unit (TCU) fails	SIM in new TCU can be provisioned to same MNO as used in the failed TCU	All possibilities	Once
	Refitting of telematics control unit	SIM in the refitted TCU can be provisioned to a relevant MNO as required	All possibilities	Once
Revision of large scale connectivity strategy	Automaker changes MNO (e.g. for commercial reasons)	Automaker can provision the SIM to a new MNO	Automaker service contract	Very infrequent
	Automaker changes business model (i.e. who pays for connectivity)	Automaker can change business model or offer free period by provisioning SIM from its MNO to/from the customer's MNO. Transfer subscription	Automaker service contract	Infrequent
	MNO merger/acquisition: MNO A	Automaker can	Automaker	Very

Process	Connectivity Use Case	Use Case Characteristics		
		Description	Owner of Connectivity Contract	Expected Frequency of Use Case
	is merged with MNO B. Automaker is currently with MNO B. Automaker changes subscription from MNO B to preferred MNO X since involvement of MNO A is not seen as beneficial.	provision SIM to new mobile operator	service contract	infrequent
	Automaker company acquisition: Automaker A buys automaker B or brand from automaker B. Subscription for bought automaker B needs to be changed to MNO from automaker A	Automaker can provision SIM to new mobile operator	Automaker service contract	Very infrequent
	Initial MNO goes out of business where automaker pays for telematics	Automaker can provision SIM to new MNO	Automaker service contract	Very infrequent

Table 12: Automaker Use Cases for Connectivity

These use cases represent the current and emerging needs of automakers. Further use cases are likely to evolve as car-sharing, for example, becomes more widespread. For instance, there will be cases in which the owner and the driver of a car are not related, raising the question of who pays for the telematics services.

12.1.4 Embedded Module Requirements and Solution Design Implications

Based on the use cases presented above, several design implications need to be considered in the selection and design of an embedded module based on the four basic types presented in this document. These implications fall into two categories – general and use-case specific.

12.1.4.1 General Automotive Sector Requirements

The following operating environment conditions apply to the capabilities and feature set of embedded modules and any associated off-module components that are designed for host devices in the automotive sector:

- Long delivery period / product availability
- Extended Temperature range: -40°C to +85°C
- Temperature and shock resistance
- Vibration resistance
- Mechanical shock resistance

There are also several automotive sector standards requirements that would need to be complied with. Among them are:

- AEC Q100 [47]: This standard relates to "Stress Test Qualification for Integrated Circuits“.

- ISO/TS 16949 [48]: Applies to the design/development, production and, when relevant, installation and servicing of automotive-related products.
- VDA 2C (German Association of the Automotive Industry) [49]: Audio performance requirements

12.1.5 Criteria Differentiating Automotive Grade Modules

Key aspects which distinguish automotive-grade modules from consumer electronic modules are listed below:

12.1.5.1 Quality and reliability, compliant with the requirements of the automotive industry

- Processes according to common automotive standards
- Defined product quality (delivery and field performance)
- Automotive-compliant manufacturing
- Advanced test reports and traceability

12.1.5.2 Robustness & extended performance

- Extended temperature range
- Extended shock resistance
- Automotive-compliant mounting technology
- Radio frequency connectors matching automotive requirements

12.1.5.3 Enhanced product offering

- Products enhancements (higher grade components and special mechanics)
- Automotive-specific features
- Over-the-air updating with management features to control quality of update
- Flexible building blocks and customization options
- Variants for specific regions

12.1.5.4 Lifecycle management

- Product availability: meeting extended lifecycles of automotive industry
- Technology transition: upgrading to next generation technology, variants with different technologies
- Component sourcing according to automotive requirements
- Ease of software updates
- Product support over lifecycle

12.1.6 Choosing an appropriate module

Clearly, automakers have to account for a large number of considerations when selecting the most appropriate communications technology to include in vehicles directly embedded. The decision-tree for selecting a technology is generally based upon:

- Services to be provided
- Regional technologies available

- The match between the services and the most appropriate regional technologies (including eventual switch-off timelines)
- Target total costs of ownership of the solution (including maintenance)
- Required duration of solutions (i.e. long life duration and capability to able to provide the components for 10 years minimum)
- Sustainability of the form factors
- Power consumption performance
- Size of the solution (in many cases, the device must be very small)

Clearly, automakers should make the appropriate selection from the beginning to avoid:

- Retrofit costs (generally more than €100)
- Difficulty in upgrading modules (requires a visit to the mechanic)
- Perceived instability of service solutions.

12.1.6.1 Why is the module choice so important?

Great pressure exists to reduce costs for telematics and infotainment services. This pressure is particularly acute given that a stable mono-mode hardware solution for most markets is impossible to guarantee for 15 years.

For this reason, the pan-european eCall regulation has generated much discussion. A module supporting both GSM and UMTS radio technologies (dual-mode) should facilitate greater flexibility in responding to different cellular network evolution paths across Europe for a longer period of time (i.e. more likely to correspond to the lifetime of the vehicle).

Please refer to the GSMA publication on Connected Cars: The Technology Roadmap (2012) for additional information on the automotive requirements and use cases for telematics and infotainment.

12.2 Consumer Electronics

12.2.1 Ecosystem Description

The ecosystem of Consumer Devices is mainly composed of the following key players as shown below:

- End-Users
- Embedded Devices Supply Chain
- Communication & Service Providers
- Application Providers
- Standard Bodies, Alliances and Regulators

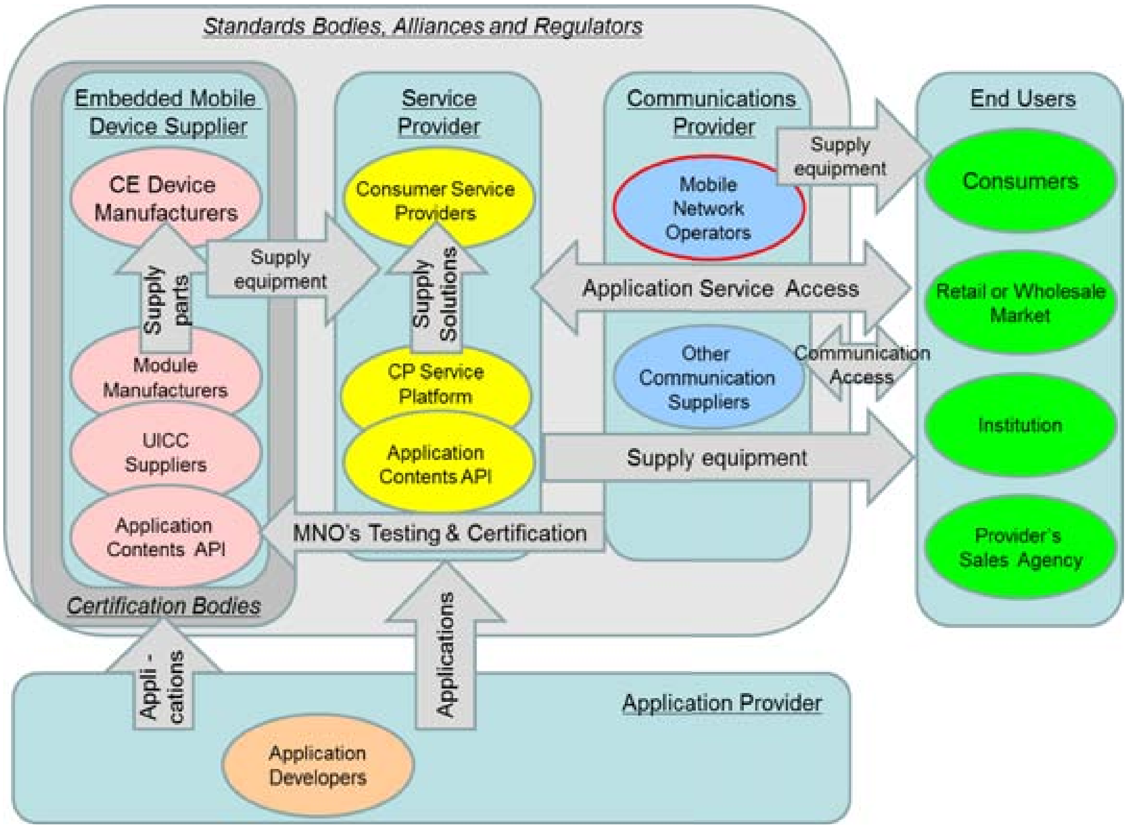


Figure 11: Consumer Electronics Embedded Mobile Eco-System

12.2.1.1 End-Users

Consumer

This is the human user who owns the connected consumer device to which the application services are being delivered by service providers. This can also refer to a machine that is used by the consumer to use the connected consumer service.

<u>Retail or Wholesale Market</u>

This is the retail store or wholesale (online/offline) markets through which the connected consumer device is sold to the consumer. Examples of this include merchants such as Best Buy and E-Bay.

<u>Institution</u>

This is the institution which has purchased a solution (which may include devices and services) for its members. For example, an educational institution such as a school may purchase connected tablets for its students. In this case, there are two sets of end users / customers – the school itself and end users such as students and teachers. This reflects a B2B2C business model.

<u>Provider's Sales Agency</u>

This is the sales agency that the communication provider or service provider owns to sell the connected consumer device to the final end user.

12.2.1.2 Embedded Device Supply Chain

<u>CE Device Manufacturers</u>

These are the supplier of consumer electronic devices to the end users, service providers and communication providers. They are responsible for integrating the embedded module, UICC and application contents API. They may have an established relationship with the service provider(s).

<u>Embedded Module Manufacturer</u>

These entities are responsible for the design, development and production of the embedded module. They work with the consumer device manufacturer to integrate the embedded module in the consumer device

<u>UICC Suppliers</u>

These suppliers are responsible for the manufacture of the UICC card. They work with the MNO to ensure compatibility with the mobile network and with the embedded module manufacturer to ensure compatibility with the embedded module.

<u>Application Contents API (Application Programming Interface) Suppliers</u>

These suppliers are responsible for providing the software to deliver application contents specific to CE devices. They work with the MNO to ensure application contents compatibility and inter-operability with the mobile network or service providers. 'Applications' in this sense refers to both platforms (for managing and serving content) and individual 'apps'.

12.2.1.3 Communication and Service Providers

<u>Mobile Network Operator (MNO)</u>

This entity provides the communication access to the service provider that is responsible for delivering application services to the end user who owns the connected, consumer electronics device. The MNO is the issuer of the UICC to the end user. In a number of instances, the MNO may also be the service provider. In some instances, the MNO may only provide the cellular service that goes with the connected consumer service. MNOs may provide wireless connectivity with licensed access technology and unlicensed access technology and also leverage their own infrastructure (for example, back-end office, Network Operating Centre). In some use cases, MNOs provide their certified integrated device to the end user directly.

Third Party Service Providers

This provider usually offers the connected consumer service to the end user, sometimes bundling the end consumer electronic device and the mobile service provider's UICC/service. They may provide expertise in integrating the connected consumer device to the MNO's IT infrastructure and back office systems. , These service providers may also integrate other 3rd party solutions into their EM service solution(s).

Application Service Provider

This entity provides the application contents API to the CE device manufacturer and the service providers. These application service providers may also be the service providers.

12.2.1.4 Standards bodies, Alliances and Regulators

This category includes standard bodies, industry initiatives and various alliance organizations that are active in setting and specifying regulatory and technical specifications for Embedded Consumer Devices and connected consumer services. It can also refer to a vertical industry body that is utilising connected devices e.g. educational authorities. Their span of influence includes: legislating the regulations; safety or conformance testing with agreed standards; and providing certification approval for the device and the service.

12.2.2 Representative Use Cases for the Consumer Electronics Sector

The following is a brief list of the use cases to be supported by the embedded modules:

- e-Book Reader
- Digital Photo Frame
- Connected Digital Cameras
- Handheld Game Consoles
- Personal Tracking and Navigation Devices
- Portable Media Players
- MP3 Players
- Tablets purchased by an educational institution and distributed to its students and teachers

In this section, the e-Book reader and digital photo frame are described as exemplary use cases of consumer devices.

12.2.2.1 e-Book Reader

E-Book readers enable books and similar reading materials to be delivered to the end user following a purchase from an online bookstore. The contents can be delivered without any limitations on the location of the end user or the time of purchase thanks to the use of cellular connectivity. The figure below illustrates the basic use case and modes of use.

Use Case	Description
	READING While sitting on the beach, moving in the transportation, and so on, the end user access the online bookstore, downloads the e-book contents (for example, Novel, Magazine) that he/she has an interest and willingly purchase and reads it.
	WRITING While the end user reads the e-book contents, he/she takes the notes directly on the margin(kind of writing/note space) of e-book reader with writing tool(for example, stylus pen, touch)
	REFERENCING and SHARING While the end user finds interesting or curious words/sentences/paragraphs/pictures on e-book contents, he/she access to the portal, blog and SNS(Social Networking Service) group to get an answer, to discuss , to share it with other users.

Figure 12: e-Book Reader Use Case

12.2.2.2 Digital Photo Frame

The digital photo frame can display digital photos, video clips and sometimes voice, SMS and e-mail content stored within internal memory or from an external storage server. The different forms of content are received by the device from other mobile devices that employ camera, MMS and e-mail capabilities over a cellular connection.

The figure below shows the basic use case for the digital photo frame. The end user takes a picture using a device with digital camera functionality and sends it to the digital photo frame directly using MMS or E-mail via a portal. The digital photo frame may include the capability to send an SMS to acknowledge receipt of the photo to the sender.

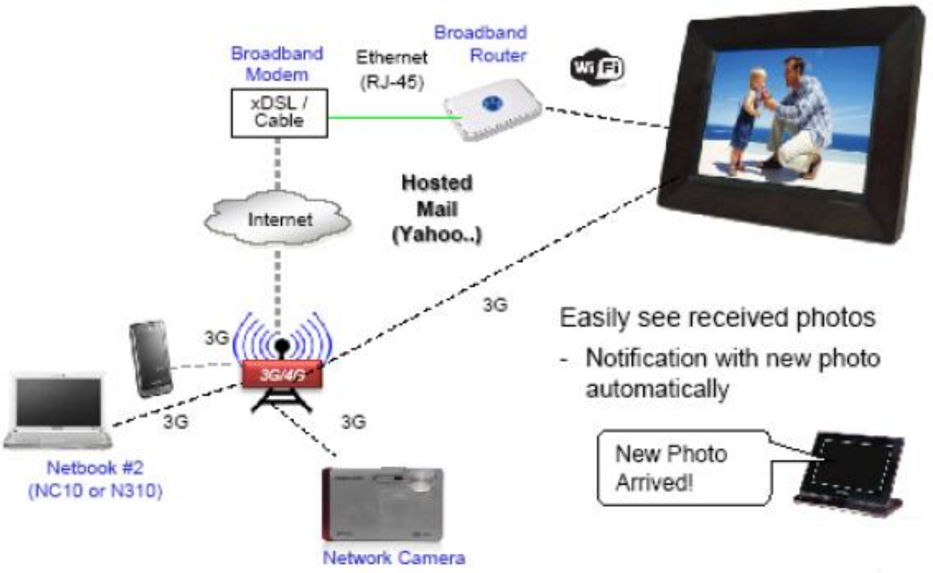


Figure 13: Digital Photo Frame Use Case

12.2.3 Embedded Module Requirements and Solution Design Implications

There are several common requirements for e-book readers, digital photo frames and similar consumer electronics devices where the small size of the device is an important product consideration. These include the following:

- Connected consumer devices should be simple for the end user to use (for example, no computer, no cables, no syncing.)
- Connected consumer devices should support 2G/3G/LTE mobile connectivity and/or Wi-Fi to download or upload the contents anywhere with cheapest cost.
- Connected consumer devices should be light and thin.
- Connected consumer devices should have long battery life.
- Connected consumer devices should support universal plug-and-play, zero-configuration, mDNS, or similar functionality
- The module in connected consumer devices should be ultra-small, ultra-slim sized to be easily embedded.
- The module in connected consumer devices should support low powered operating modes.
- The module in connected consumer devices should support work to be completed off-line with synchronisation occurring when the user ranges back in to network range.

12.2.4 Mobile Education Reference Documents

- The Mobile Proposition for Education: http://www.gsma.com/documents/the-mobile-proposition-for-education/21359

12.3 M-Health

The focus of this section is on the development of m-Health guidelines that will become common across the healthcare industry and will be equally applicable for the most part across all healthcare OEMs

12.3.1 Ecosystem Description

The ecosystem of m-Health is mainly composed of the following key players as below:

- End-Users
- Application Service Provider
- Embedded Device Supply Chain
- Communication and Service Providers

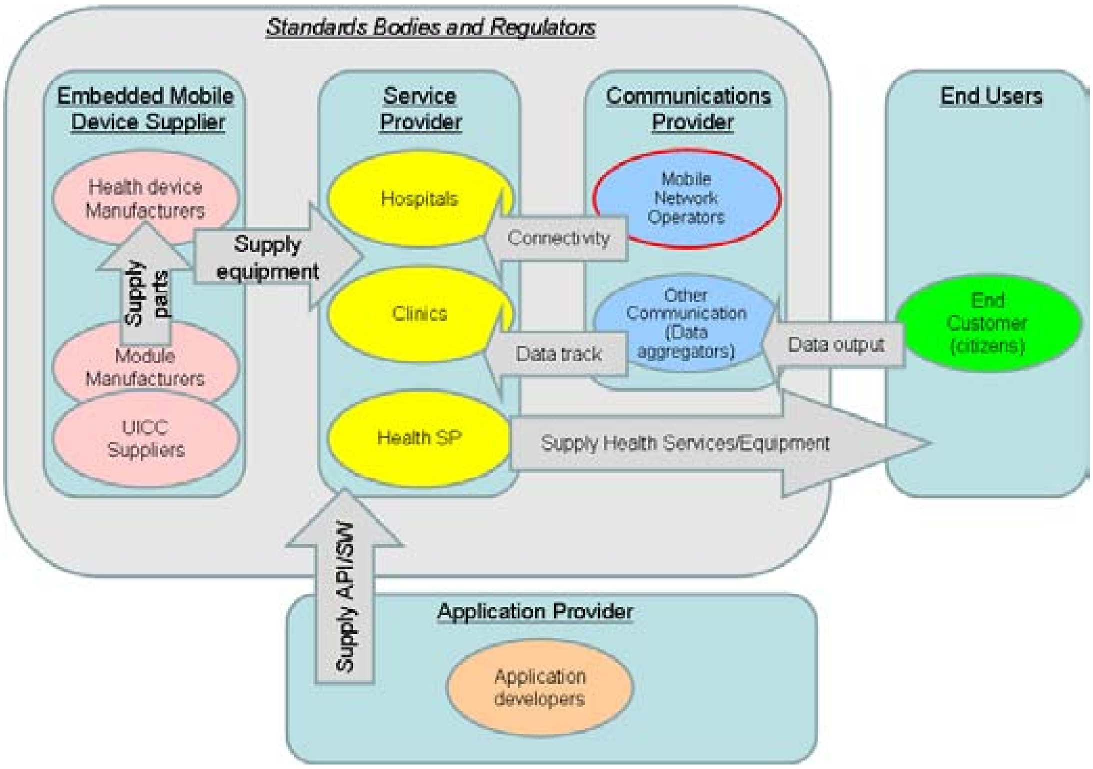


Figure 14: mHealth Embedded Mobile Eco-System

Error! Reference source not found. The figure above illustrates the m-Health ecosystem. It is a B2B2C market, where the role of the MNO is to provide connectivity/ basic services to other companies that sell a health service to end-users.

An application provider, which is typically the owner of the m-health application, provides its application(s) to service providers, such as hospitals, medical clinics and care centres. service providers offer m-Health services that operate with an embedded module inside a host device.

12.3.1.1 End-User

End-User /Consumer/Patient/Medical Professional

An end user of an m-Health service can either be a consumer, patient, medical professional or care giver using the device.

12.3.1.2 Communication Service Providers

Mobile Network Operator (MNO)

MNOs can have the following roles within the m-Health ecosystem:

- Establish and provide connectivity,
- Provide additional value-added services (for example, billing, data storage, device management, identity management)
- End to end healthcare service provider

Healthcare Service Provider

Healthcare service providers are responsible for managing the services, m-Health applications, devices and commercial tariff plans to end-users. Healthcare service providers have a direct relationship with MNOs and application service providers.

Application Service Provider

These are typically the owners of application(s) that support the embedded service (for example, API, IPR, software). Application service providers will typically have a commercial agreement with the communication service provider to deliver the service.

12.3.1.3 Embedded Device Supply Chain

Embedded Device Suppliers

These suppliers have a direct relationship with MNOs for the supply of hardware (for example, UICC, embedded device, embedded module).

Embedded Module Vendor

Provides embedded modules for embedded devices within the requirements and/or specifications issued by standards bodies and governmental agencies

Embedded Device Manufacturer

Provides host devices within which the application runs.

UICC Manufacturer

Provides UICC that MNOs manage to provide connectivity to the service

Further explanation of ecosystem roles and business models can be found within the GSMA/AT Kearney 2011 paper 'Mobile Health, Who pays'[5] which provides detailed analysis into Mobile Health Reimbursement and Business Models,

[5] Mobile Health, Who pays' GSMA and AT Kearney 2011

12.3.2 Medical Device Regulation

Medical device regulations were initially developed to safeguard users against harm from using the device, classifying devices according to the relative risk that they pose, with greater controls being applied to higher risk devices. M-Health involves connecting these devices in ways that were not foreseen when they were classified, essentially connecting up a number of components to provide an overall service. The safety and effectiveness of a service involving embedded m-Health capabilities can only be fully understood by considering the full end to end system. Medical device regulations are therefore a critical consideration when developing mobile health solutions.

"Intended Use" is a cornerstone of device regulation

Medical device regulations, whilst broadly similar, do vary from country to country. However, a governing principle in medical device regulation in both EU and US is that of "Intended Use". Any determination regarding applicability of medical device regulations to a product or service will be based on the intended purpose of the product and its mode of action.

Considering a product's intended use in conjunction with the regulators definition of what constitutes a medical device (discussed later) enables manufacturers to decide with reasonable clarity, whether the product will fall within the scope of the regulations where there are no claims made regarding the suitability of a network or a mobile device for medical purposes, then this principle should generally relieve both mobile network operators and vendors of mobile communications equipment of any burden in medical device regulation.

There is ample guidance available to manufacturers on FDA (USA) and MHRA (UK) topic, and many other aspects of device regulation. The figure below summarises how the high-level risk landscape changes depending on the use of the m-Health device.

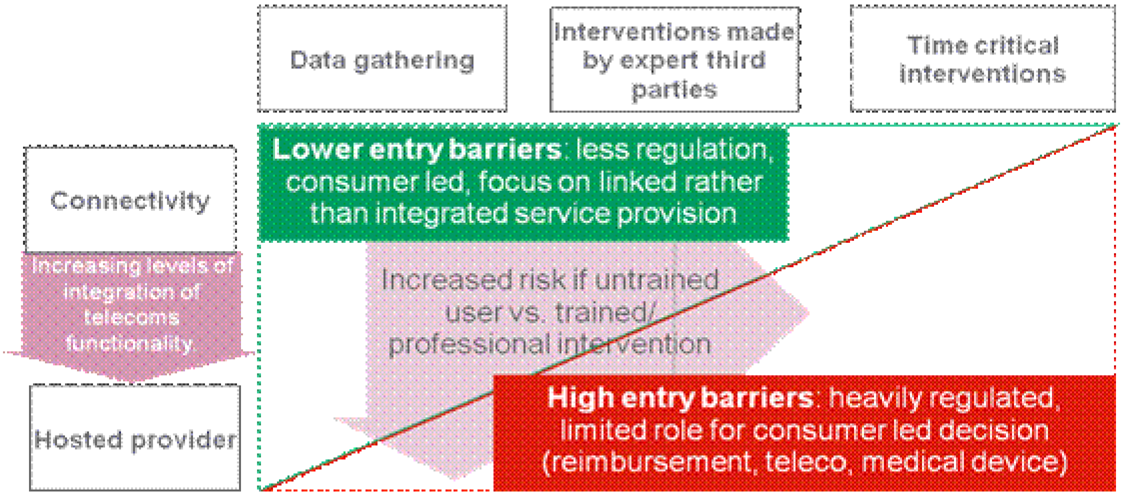

Data gathering
Interventions made by expert third parties
Time critical interventions
Connectivity
Increasing levels of integration of telecoms functionality
Hosted provider
Lower entry barriers: less regulation, consumer led, focus on linked rather than integrated service provision
Increased risk if untrained user vs. trained/ professional intervention
High entry barriers: heavily regulated, limited role for consumer led decision (reimbursement, teleco, medical device)

Figure 15: How Regulation changes depending on the intend use of a device

12.3.2.1 Risk Assessment and Medical Device Classification

Medical devices by their very nature have the potential to present a hazard - to be a source of harm in normal use, and more so if misused. Regulations are therefore a necessary instrument to safeguard users from undue and unnecessary risks and are based on the principle of mitigating, to an acceptable level, the potential of a device to cause harm.

Determination of the potential to cause harm (risk assessment) and implementation of appropriate risk reduction measures through the design and development process is an essential requirement under the regulations.

Regulators recognize that there are many different types of medical devices with a correspondingly wide range of associated risk. Medical devices are therefore assigned to a particular class (national regulations typically identify three or four device classes). The classification is made according to a set of rules within the regulations and is based on device design complexity, use characteristics, and potential for harm in normal use and foreseeable misuse situations. The extent to which regulatory controls are applied varies progressively from class to class, in proportion to the potential hazard they present.

The regulations acknowledge that:

- Absolute safety cannot be guaranteed
- It is a risk management issue
- It is closely aligned with device effectiveness/performance
- It must be considered throughout the life span of the device

Regulations place obligations on manufacturers, but also provide a supporting framework for product development, facilitating design and development of products that are for fit for purpose and that provide an acceptable risk-benefit balance.

12.3.2.2 Standards

The use of standards has been a key element in establishing medical device regulations. The International Organization for Standardization (ISO) defines a standard in the medical device domain as follows:

"Standards are documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines or definitions of characteristics, to ensure that materials, products, process and services are fit for their purpose".

Standards can establish a wide range of specifications for products, processes and services

- Prescriptive specifications obligate product characteristics, e.g. device dimensions, biomaterials, test or calibration procedures, as well as definitions of terms and terminologies.
- Design specifications set out the specific design or technical characteristics of a product, e.g. operating room facilities or medical gas systems.
- Performance specifications ensure that a product meets a prescribed test, e.g. strength requirements, measurement accuracy, battery capacity, or maximum defibrillator energy.
- Management specifications set out requirements for the processes and procedures companies put in place, e.g. quality systems for manufacturing or environmental management systems.

Prescriptive design and performance specifications have been commonplace in standards for some time and management specifications have also rapidly gained prominence. Recent years have seen the development and application of “generic management system standards”, where “generic” means that the standards’ requirements can be applied to any organization, regardless of the product it makes or the service it delivers, and “management system” refers to what the organization does to manage its processes.

Two of the most widely known series of generic management system standards are the ISO 9000 series for managing quality systems, and the ISO 14000 series for environmental management systems. ISO13485 and ISO13488 are specific ISO quality systems standards for medical device manufacturing. As indicated earlier, there is wide ranging information and assistance relating to these standards and their application available on regulatory and standards organizations websites.

12.3.2.3 The Role of the Manufacturer

The term 'Manufacturer' has specific meaning within medical device regulations and is worthy of clarification here owing to the potential for misinterpretation. 'Manufacturer' means the legal company with responsibility for the design, manufacture, packaging and labelling of a device before it is placed on the market under the company name, regardless of whether these operations are carried out by that company itself, or on their behalf by a third party.

Put simply, if you or your company place a medical device on the market, you or your company are the legal manufacturer and you are thus responsible for compliance with the applicable medical device regulations. This is true, irrespective of what your route to market is - the distributor, for example, has no responsibility here. In addition, as the manufacturer, you are responsible for post-market surveillance; monitoring and acting upon any adverse events or complaints in the field. It must be clear to the consumer therefore, how they can contact the manufacturer (again, not the distributor) in order to report such events.

12.3.2.4 Device, Accessory and Component

Beyond intended use, regulators make a distinction between a medical device, an accessory and a component; each of which is regarded and managed differently in the regulations. The elements of a mobile health solution may include sensors, software, a mobile phone and an associated network infrastructure, each of which could be classified as a device, accessory or component, depending on the construction of the specific product and the intended use. Understanding the distinction is key to navigating the healthcare regulations

12.3.2.5 The distinction between Wellness and Healthcare

As consumers in developed economies take a more active role in managing their own health, overall lifestyle choices are increasingly identified as a major contributor to health and well-being. As a result, more products are appearing on the market promoting 'wellness' and the determination of whether a product falls within the scope of medical device regulations can be challenging as the boundaries between wellness and healthcare become blurred.

More detailed information on this topic can be found in the GSMA paper ‘Mobile Health Device Regulation, available at www.gsma.com/health.

12.3.3 Medical Device Interoperability and messaging standards

The need for interoperable, global standards across the healthcare industry is critical to the development and subsequent adoption of m-Health solutions. In order to achieve this, a number of organisations are looking to define robust standards for an m-Health Ecosystem that enables devices to seamlessly communicate with Healthcare systems. One of the more mature established organisations in this domain is the Continua Health Alliance (continuaalliance.org) which was founded to address this issue and whose mission is to promote interoperability of m-Health devices and provide certification to ensure compliance to the standards defined by organisations such as IEEE, HL7 & IHE.

12.3.4 Telecoms regulation

M-Health devices will be subject to all the standard telecom’s regulation in areas such as Legal Intercept, Numbering and Termination (if relevant). With regard to SAR testing m-Health devices will be subject to the same criteria as a mobile phone, and in particular the regulation that related to ‘Body Worn Devices’.

12.3.5 Representative Use Cases for the M-Health Sector

There are number of different ways that an embedded m-Health device will interact with a mobile network. Due to the vast number of different m-Health devices that are entering the marketplace, the GSMA has produced a number of representative use cases that illustrate intended to look at mHealth from a mobile network/operator point of view and should be seen as complimentary to other Use Cases that already exist from other parts of the Industry, such as the Continua Health Alliance.

12.3.5.1 Use Case 1 – One-way Direction information transfer

Patient driven healthcare – for example monitoring with automatic collection, transfer and storage to personal health records based on user choice. This could also be a prescribed activity but is always a one direction service

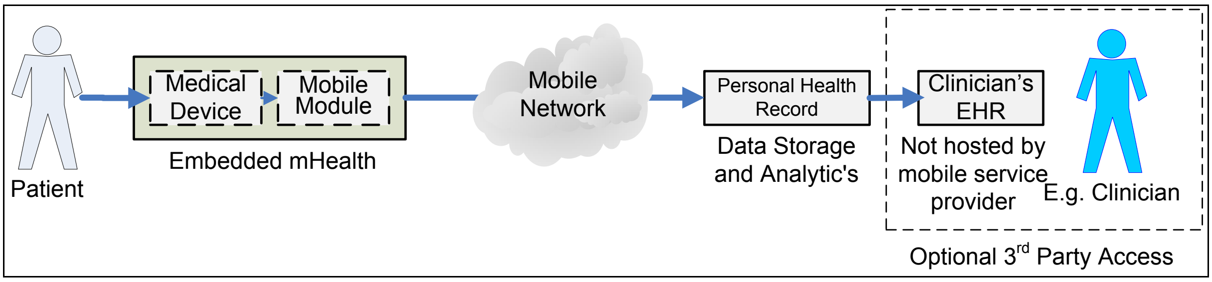


Figure 16: m-Health – One-way Direction Transfer Use Case

<u>Example: Wellness (prevention, worried well, fitness, sports)</u>

User driven wellness monitoring - Daily updates to centralised database for user access

- Device(s) used to track the activity of a user and these readings would be uploaded to a service provider on a daily or regular basis.
- User may grant access to 3rd parties like General Practitioner (GP), Clinician, fitness tracking provider as required
- User will have access to their personal data via web/PC/mobile. .

<u>Example: Remote Monitoring (post-treatment and chronic disease tracking)</u>

Health care devices such as blood pressure, medical implants, and glucose monitoring devices are used on a daily basis to monitor and track patient readings. These readings would be uploaded to a monitoring service accessed by doctors, specialists in charge of care or other authorized users.

12.3.5.2 Use Case 2 - Two-way Direction information transfer

Patient driven or prescribed healthcare with a feedback loop between the device and the service backend for example bi-directional communication between device and medical service provider (manual or automatic) based on readings taken and uploaded.

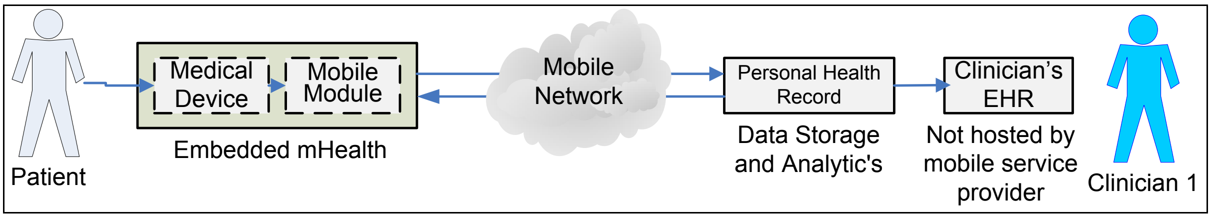


Figure 17: m-Health – Two-way Direction Transfer Use Case

Example: Remote Management (glucose monitoring, life coaching - non life threatening)

Device(s) that monitor a patient's condition and then adjusts their level of medication or behaviour coaching depending on the results supplied by the device. The assessment of the results is completed by a patient's clinician or by automatic analytic's within the backend of the service.

12.3.5.3 Use Case 3 – Quality of Service and Location-Based Services

Quality of service (QoS) and location-based services (LBS) monitoring devices will require rapid and resilient delivery of data and the transfer of location information.

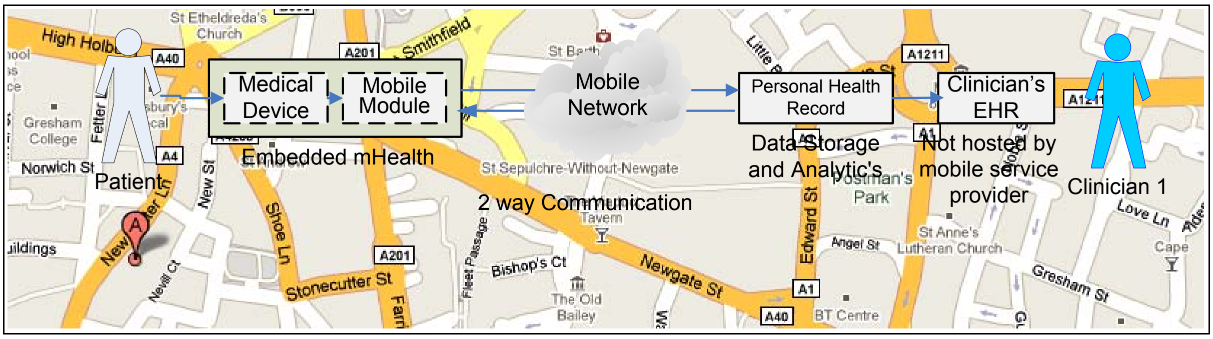


Figure 18: m-Health – QoS and LBS Use Case

Example: Emergency Alarms

Personal alarms could be carried by vulnerable individuals. If they are in an emergency situation then they will use the device to raise the alarm to a responsible person or central service centre, or the alarm will be automatically triggered in the event of an incident such as a fall. Where possible these alarms should be assigned a higher priority delivery on a mobile network, to try and ensure connection on congested cells

12.3.5.4 Use Case 4 – Multiple Patients

Clinician operated remote diagnostics where a medical professional aids a user in the use of local medical device(s)

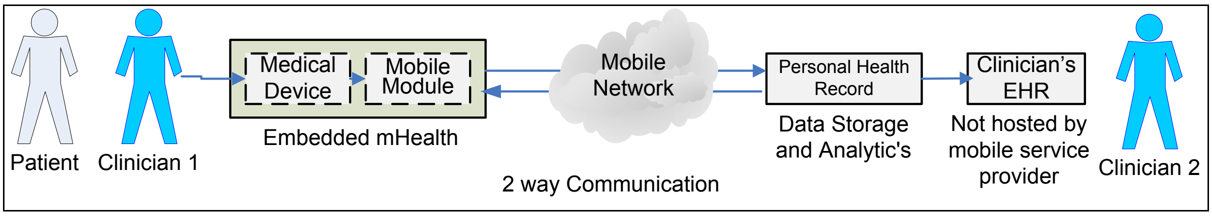


Figure 19: M-Health – Multiple Patients Use Case

Example: Remote assisted consultation

A mobile device may be used by a medical professional in the field to enable remote consultations with experts in a remote location such as a specialist medical centre.

Along with these embedded sensor devices, there is also a use case for m-Health gateways that allow medical sensors to connect using transport technologies such as Bluetooth, Zigbee and Ant + to a GSM hub that acts as a connection into the cloud. These hubs can either be personal mobile devices carried by individuals in a form factor similar to a watch or static device that is similar to a home hub.

12.4 Smart Metering and Smart Home

12.4.1 Ecosystem Description

The smart metering and smart home ecosystems are mainly composed of the following key players as below:

- Application Provider
- Communication and Service Providers
- Embedded Device Supplier (including smart meters, home gateways, connected appliances and other connected home devices)
- End-User
- Standards, Regulatory and Certification Bodies

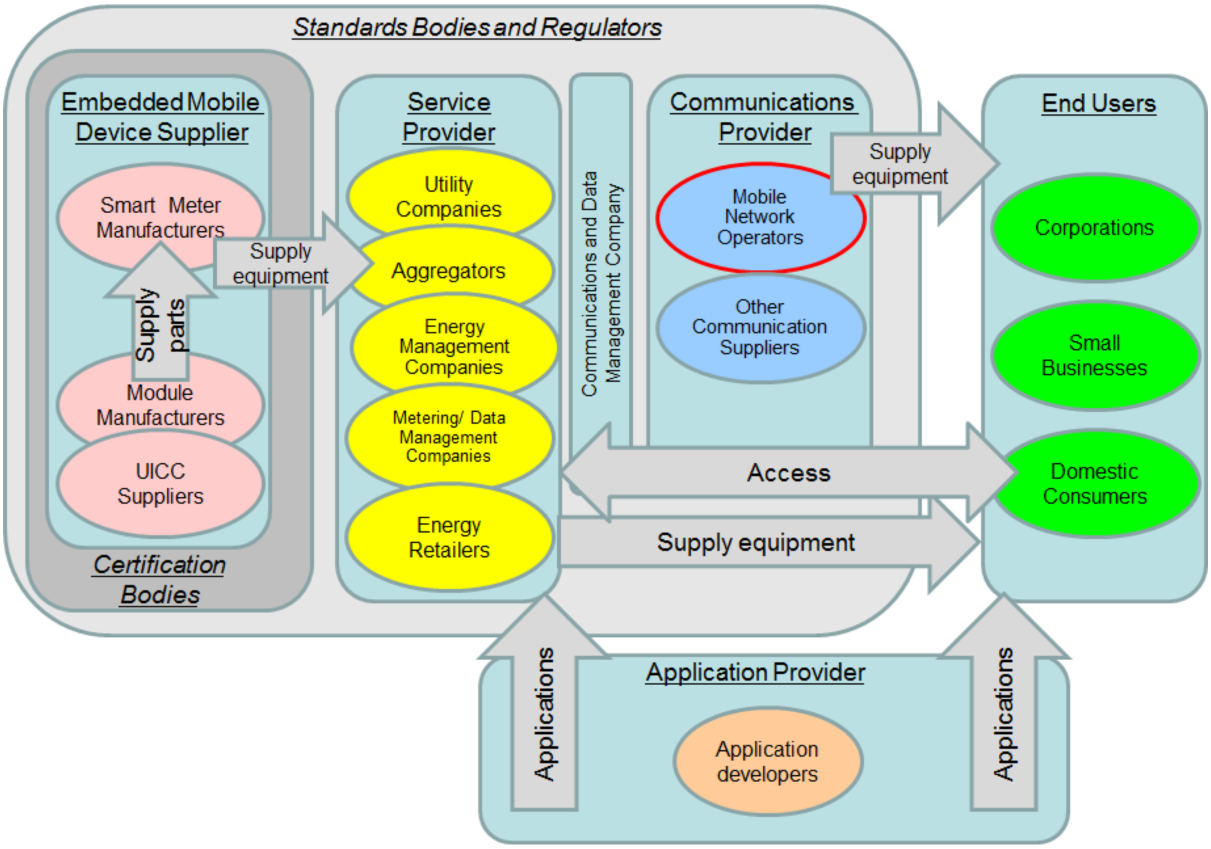


Figure 20: Smart Metering Embedded Mobile Eco-System

The two eco-systems for smart metering and smart home can be completely different, for example, when utility companies provide smart meter data reading services, and various third parties provide home energy management services. In other cases, these ecosystems can overlap significantly, for example, when energy service providers offer both smart meter data reading services as well as home energy management services (for example, demand response) to their end-users.

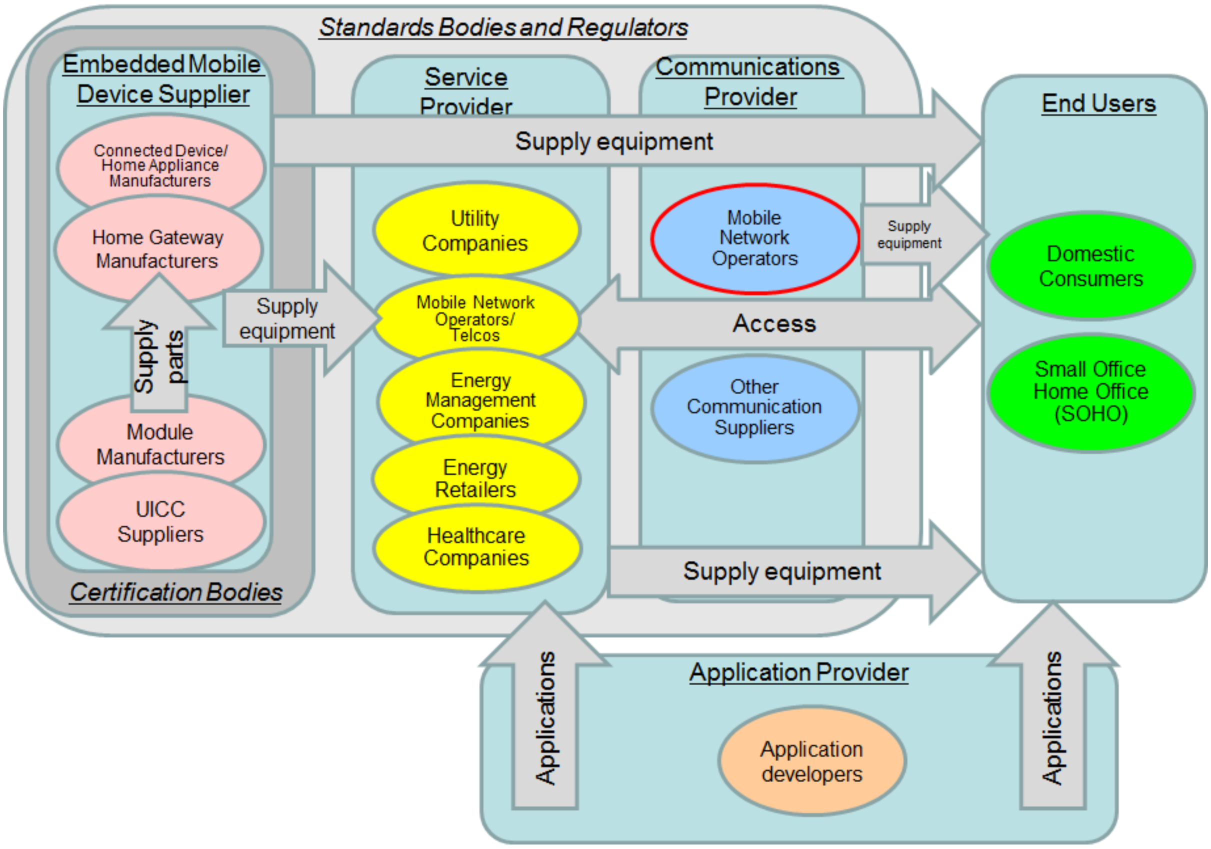


Figure 21: Smart Home Embedded Mobile Eco-System

12.4.1.1 Application Provider

The application provider could produce applications to be used by the service provider, communications provider and possibly the end-user. It may provide the skills and applications necessary to manage the smart meters and the home gateways, or manage the data and provide suitable IT applications. It may also provide end-user interface software for viewing and managing home energy consumption.

12.4.1.2 Communications and Service Providers

Communications Provider

This entity supplies the means of communication between the service provider and the End-user. The communication provider could be a mobile network operator, a fixed line operator or another type such as powerline provider, cable operator and so on. For the purposes of this document, it is assumed that the communications provider is a mobile network operator (MNO) that can provide wide-area communication using 2G, GPRS or 3G for example, UMTS based communications.

The role of the MNO in the ecosystem will be principally to provide communications access between the end user and the service provider, however, there may be value added services that could be provided. For example, the MNO can itself be a provider of energy management services in the smart home. The MNO could also take the role of an aggregator or energy management company for business customers. The MNO could be a provider of the home gateway device to the residential users.

The value of the MNO as the communications provider is expertise, universal availability, reliability and flexibility to add, remove or reconfigure multiple devices, as well as ability to collect, aggregate and manage large volumes of usage data.

The major challenge for the MNO is to provide reliable communications to a very large number of devices that communicate unpredictably. Each smart meter or smart home device does not need to be connected to the communications network for most of the time and will connect only periodically. However, the MNO does need to ensure that it can handle a very high number of periodic connections without congestion that will affect service to the connected smart meters and smart home devices, and to its other mobile customers.

Other Communications Providers

These entities supply local area network and neighbourhood network connectivity. These could be a mobile network operator or a separately licensed communications provider.

Service Providers

This term covers a number of different entities as follows:

- Utility Company. Typically the energy supplier such as the gas, electricity and water supply companies. It may also be the supplier of the smart meter to the end-user and it also communicates with the smart meter to obtain readings and perform maintenance or other checks or provide information to the end-user.
- Energy retailer that may sit between the utility companies and the end-user. It would buy energy wholesale and sell retail. It also may be responsible for administering the smart meter instead of the utility companies.
- Aggregator that may sit between the utility company and the end-user. It would be used typically for a large business with many sites that requires all its energy use managed on its behalf by a 3rd party. The mobile network operator could play the role of aggregator.
- Energy management company that may use an intelligent device or control panel other than a smart meter to collect home or business usage data and control the usage of energy consumption and the behaviour of home appliances.
- Metering/data management company that may collect meter data for the energy retailer and utility company. It would communicate with the smart meter and may also supply the meter.
- Healthcare company that may use the electricity usage data from sensors installed in the smart home as a basis for its assisted living services to the elderly, disabled, and other categories of patients.

Communication and Data Management Company

A separate entity might be established to provide a centralised collection and distribution of data from smart meters, and be responsible for the rollout of smart meters, as is the case of DCC (Data and Communication Company) set up to manage the smart metering rollout in the UK.

12.4.1.3 Embedded Mobile Device Suppliers

This covers the manufacture and supply of embedded modules, USIMs, smart meters, home gateways, home appliance and other devices with embedded mobile connectivity. There will be different manufacturers and suppliers that will work together to produce the end product. This could be a smart meter with an EM module complete with USIM or maybe where the USIM is supplied by the MNO. In the case where a hub is used to connect to multiple smart meters in the end-user’s premises, the embedded module and USIM could reside in the hub and provide connectivity for all the smart meters and other devices. In the case where there is a gateway/concentrator to which connect smart meters from a number of end-users' premises, the embedded module and USIM could reside in the gateway/concentrator.

12.4.1.4 End-User

This is the consumer of services from the service provider and who has the smart meter installed in the premises. This could be a domestic user or a small, medium or large business user. The end-user may have a direct commercial relationship with the service provider (in particular the utility company) and would probably have no direct relationship with, and may be completely unaware of, the communication provider. Alternatively, home control and monitoring services could be provided to the end-users directly by the communication provider.

12.4.1.5 Standards, Regulatory and Certification Bodies

The standards bodies produce appropriate standards for the embedded modules, USIMs smart meters and the communication protocols between them. These standards will govern the operation in the supplier, manufacturers, service providers and communication providers. The regulatory bodies will govern the use of these systems, particularly in relation to their operation. The certification bodies will ensure that the devices are fit for purpose and operate in accordance with regulatory and standards.

The general smart metering and smart home architecture is shown below. This shows the elements and their interconnection between different entities. note that smart meters in the end-user's premises could have their own communication module embedded or could be connected to a communications hub in the end-user's premises that has the embedded communications module. Alternatively, a number of smart meters could be connected via a neighbourhood area network to a gateway/concentrator that has the embedded communication module.

Other devices such as smoke alarms, heating control systems, and other home appliances, such as refrigerators and washing machines could be connected to an energy management system in the end-user's premises that connects to a "lifestyle communications hub" (unregulated). For regulatory and security reasons, this hub is completely separate from the hub that connects the smart meters.

The smart metering service providers could all have separate relationships with the end-users; it is also possible that a central body is established for collecting and managing the data, as for example, in the case of the UK. The Data Communication Company in the UK will manage contracts with communications and data providers on behalf of the utilities service providers.

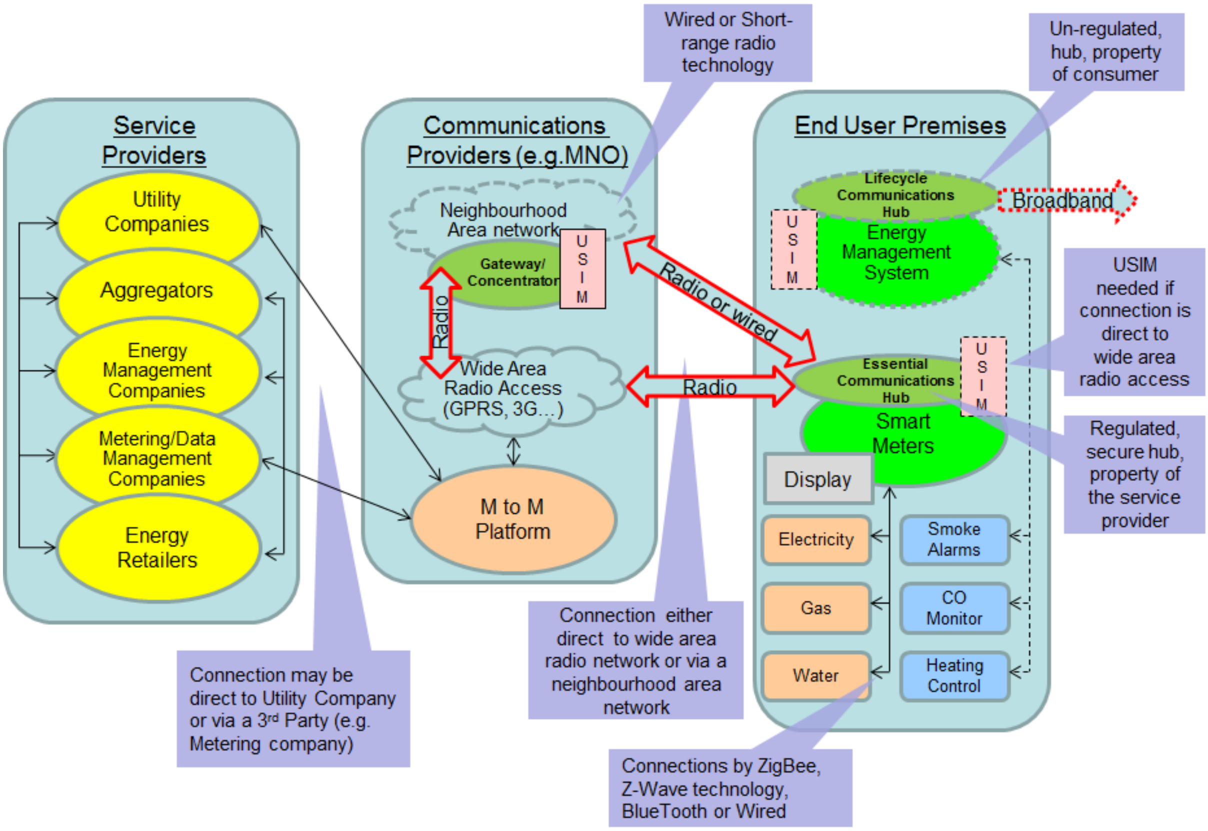

Service Providers
Utility Companies
Aggregators
Energy Management Companies
Metering/Data Management Companies
Energy Retailers
Communications Providers (e.g.MNO)
Neighbourhood Area network
Gateway/ Concentrator
USIM
Radio
Wide Area Radio Access (GPRS, 3G…)
M to M Platform
End User Premises
Lifecycle Communications Hub
Energy Management System
USIM
Broadband
Radio or wired
Radio
Essential Communications Hub
USIM
Smart Meters
Display
Electricity
Gas
Water
Smoke Alarms
CO Monitor
Heating Control
Wired or Short-range radio technology
Un-regulated, hub, property of consumer
USIM needed if connection is direct to wide area radio access
Regulated, secure hub, property of the service provider
Connection may be direct to Utility Company or via a 3rd Party (e.g. Metering company)
Connection either direct to wide area radio network or via a neighbourhood area network
Connections by ZigBee, Z-Wave technology, BlueTooth or Wired

Figure 22: Architectural Relationships for Smart Metering Use Cases

The two sub-sections below list use cases for the smart metering and smart home sectors. There are many other use cases that require the use of the embedded modules and mobile connectivity, most notably use cases for smart grid and smart cities. These will be described in the next release of the Embedded Mobile Guidelines.

12.4.2 Representative Use Cases for the Smart Metering Sector

Possible use cases to be supported by the embedded modules include:

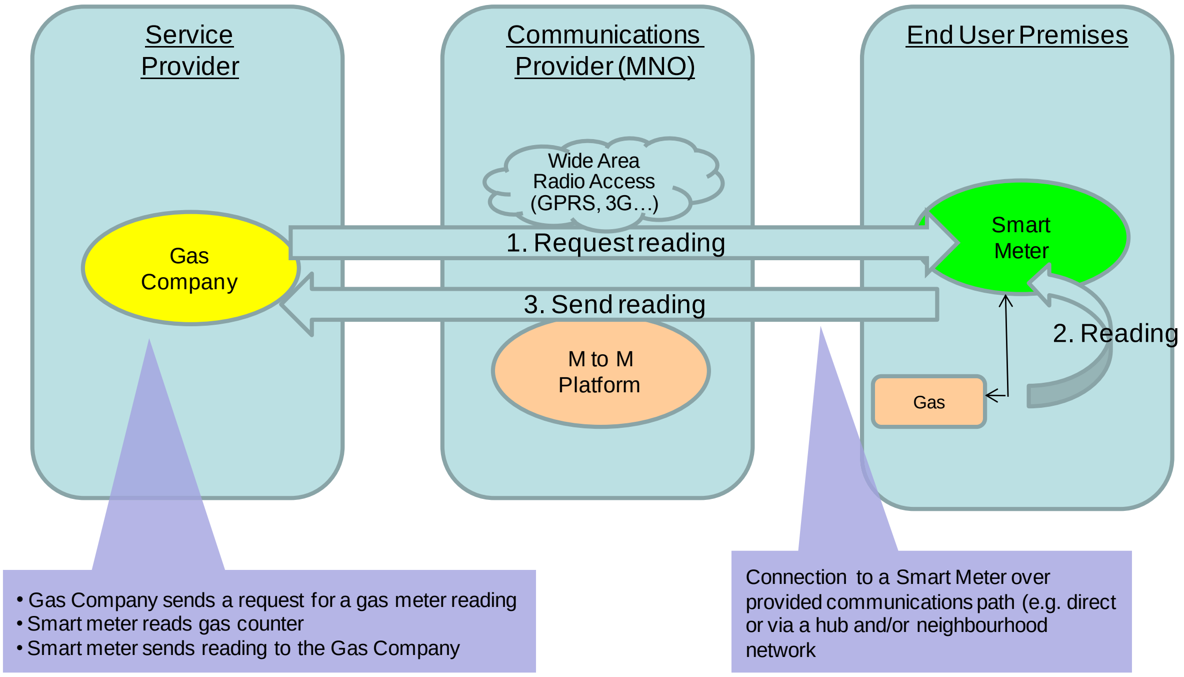
- Provide periodic or on-demand meter reads
- Remote end-user control of systems
- Provision of information to the end user
- Energy consumption management for multiple business locations or a single home location
- Administration of prepaid metering
- Support for advanced tariffing methods, for example time of use tariffs
- End user equipment monitoring and management
- Meter alert and diagnostic
- Smart meter software upgrade.

More information is available in the ETSI document TR 102 691 of which the use cases above are a sub-set. The smart metering functionality and use cases are also developed by the CEN/CENELEC/ETSI Smart Meter Co-ordination Group (SMCG). The CEN/CENELEC Energy Management working group is designed to initiate a European collective view of the general strategy for improvement of energy efficiency standardisation and to set an agreement between all CEN/CENELEC members on the objectives to achieve.

Some of the above use cases are shown in more detail below:

12.4.2.1 Periodic or on-demand meter reads

The service provider (in this case the gas company) wants to read the customer's gas meter remotely. The command is sent to the customer's smart meter using the communication service provided by the mobile network operator. The reading is sent back to the gas company over the same communication path. The role of the MNO in this case is just to provide the communication between the service provider and the end-user.



- Gas Company sends a request for a gas meter reading
- Smart meter reads gas counter
- Smart meter sends reading to the Gas Company

Connection to a Smart Meter over provided communications path (e.g. direct or via a hub and/or neighbourhood network

Figure 23: Use Case On demand Remote Meter Reading

12.4.2.2 Remote end-user control of systems

The end-user wants to switch on his heating in his house. He does this by using a command sent from his mobile device. The command is sent over the wide area radio network to an energy management company that sends the command over the wide area radio network to the lifestyle communication hub at the user's house. This then sends the command to the heating control. An acknowledgement is sent to the end-user that the heating has been switched on. The role of the MNO in this case is to provide the communication between the end-user and the energy management company and between the energy management company and the home lifestyle communication hub.

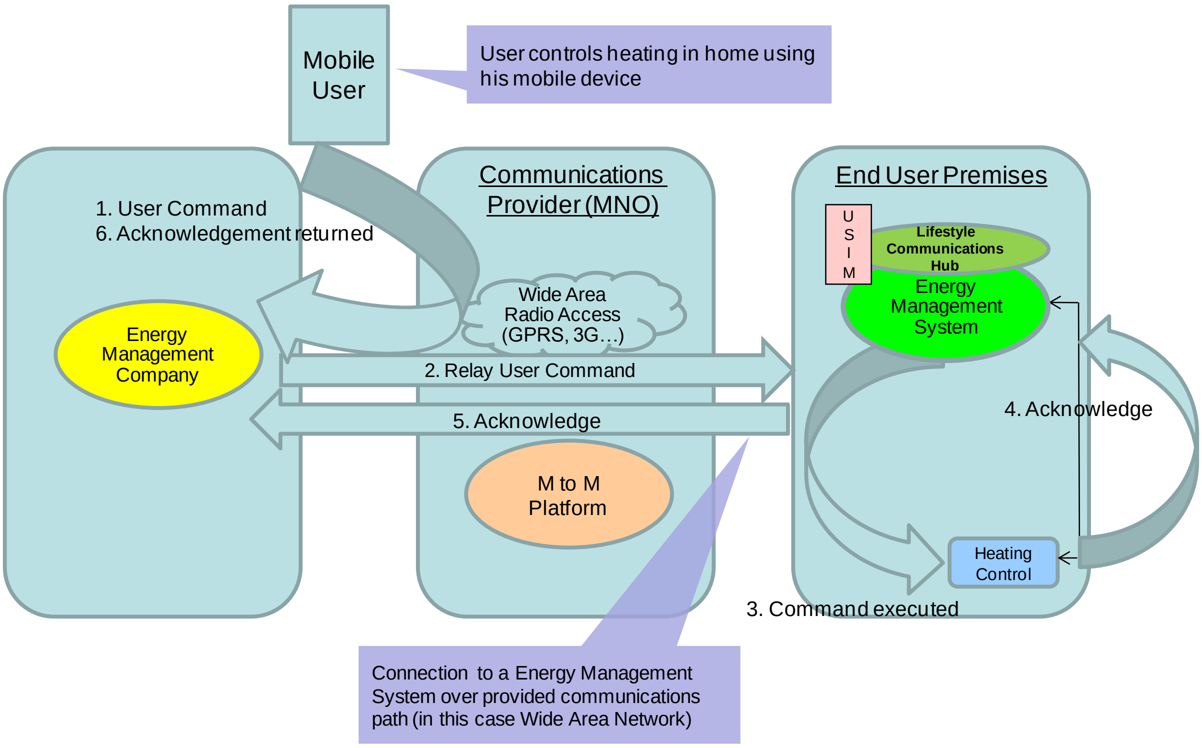

Mobile User
User controls heating in home using his mobile device
1. User Command
6. Acknowledgement returned
Energy Management Company
Communications Provider (MNO)
Wide Area Radio Access (GPRS, 3G…)
2. Relay User Command
5. Acknowledge
M to M Platform
End User Premises
USIM
Lifestyle Communications Hub
Energy Management System
4. Acknowledge
Heating Control
3. Command executed
Connection to a Energy Management System over provided communications path (in this case Wide Area Network)

Figure 24: Use Case Remote End-User control

12.4.2.3 Provision of information to the end user

the utility company wants to inform the customer that his heating system is ready for a service and invites him to make an appointment. The message sent using the communication service provided by the mobile network operator and is shown on the display on the on the smart meter with an in-home display. Alternatively, it could be sent to the display on an energy management system connected via the lifestyle communications hub or. The role of the MNO in this case is just to provide the communication between the service provider (energy management company) and the end-user.

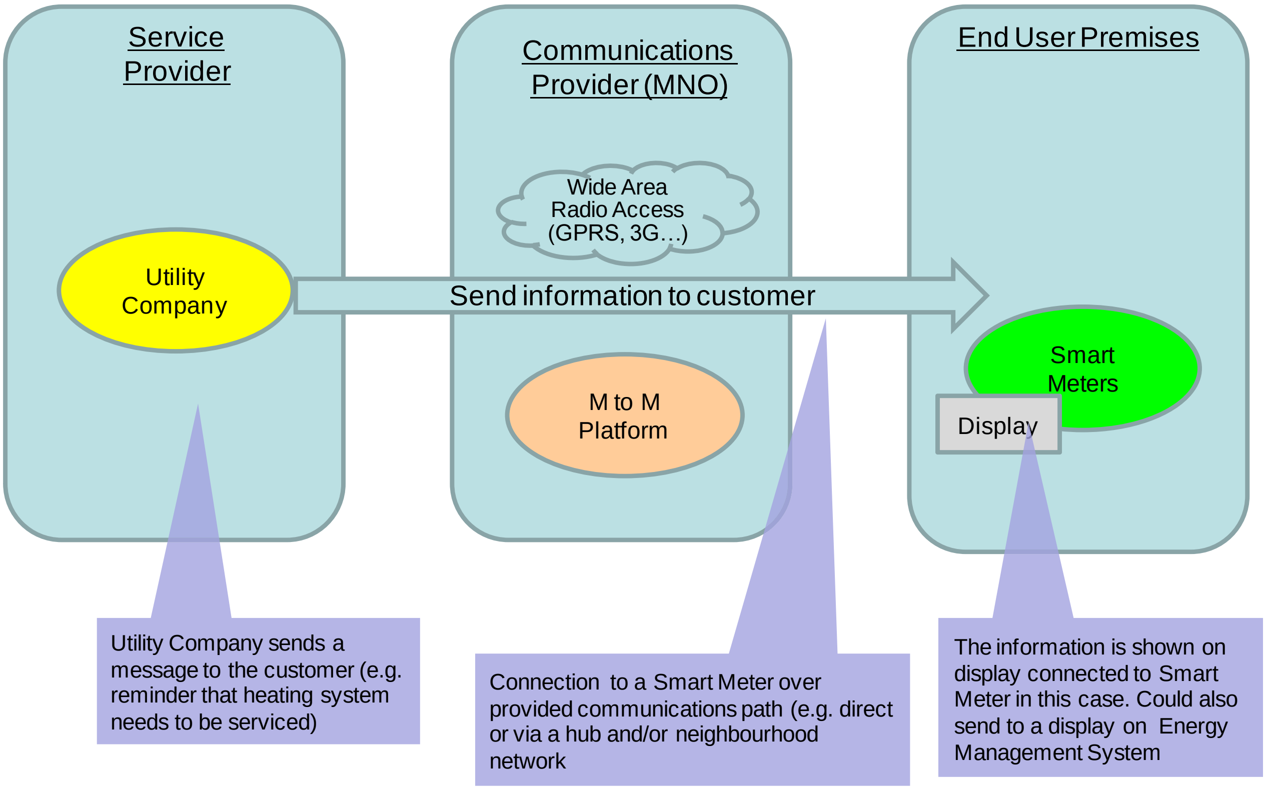

Service Provider
Communications Provider (MNO)
End User Premises
Wide Area Radio Access (GPRS, 3G…)
Utility Company
Send information to customer
Smart Meters
Display
M to M Platform
Utility Company sends a message to the customer (e.g. reminder that heating system needs to be serviced)
Connection to a Smart Meter over provided communications path (e.g. direct or via a hub and/or neighbourhood network
The information is shown on display connected to Smart Meter in this case. Could also send to a display on Energy Management System

Figure 25: Use Case Information sent to the End-User

12.4.2.4 Energy Consumption Management - Large Business Customer

A large company has its energy use monitored and controlled remotely. This is done by an “aggregator” (which can also be called building or energy management company) that collects readings from all the premises of the company and may pass the information to the utility companies (or receives data from the utility). the utility companies (or the aggregator) have information on the energy usage of the end-user and can follow the usage pattern and adjust if required within an agreed profile. The role of the MNO in this case is to provide the communication between the aggregator (or energy/building management company) and the smart meters and the energy management system in the business premises. Additionally, the MNO could play the role of the aggregator/energy management company.

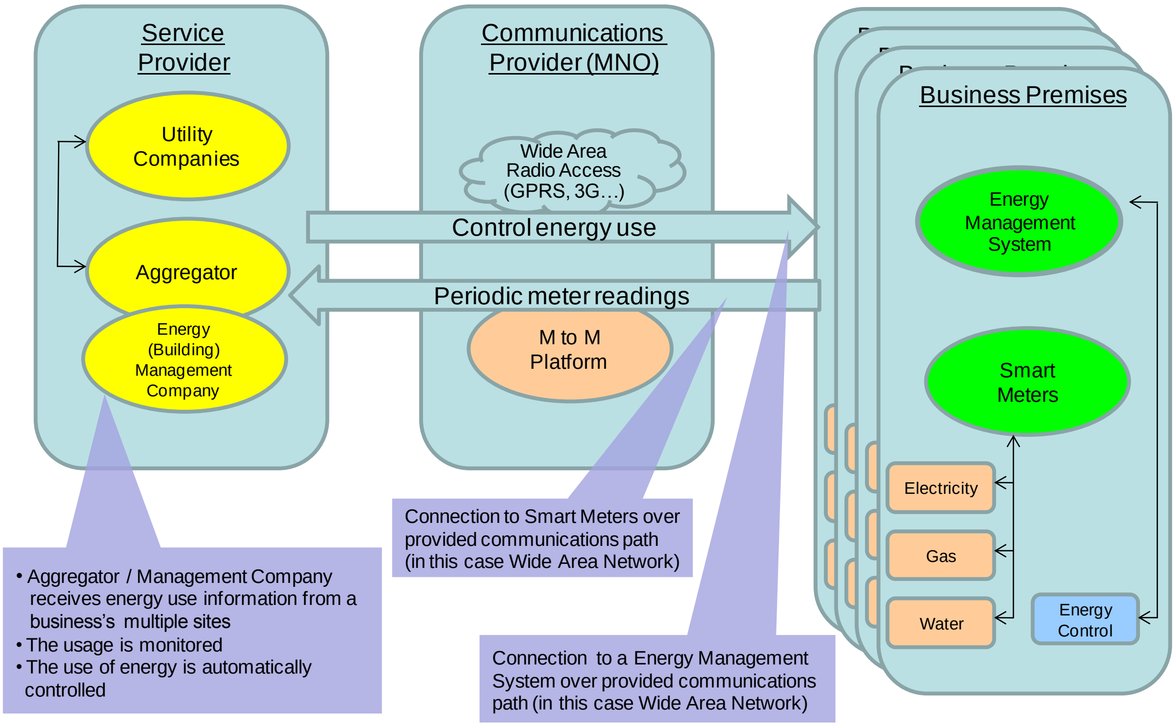

Service Provider
Utility Companies
Aggregator
Energy (Building) Management Company
Communications Provider (MNO)
Wide Area Radio Access (GPRS, 3G…)
Control energy use
Periodic meter readings
M to M Platform
Business Premises
Energy Management System
Smart Meters
Electricity
Gas
Water
Energy Control
• Aggregator / Management Company receives energy use information from a business's multiple sites
• The usage is monitored
• The use of energy is automatically controlled
Connection to Smart Meters over provided communications path (in this case Wide Area Network)
Connection to a Energy Management System over provided communications path (in this case Wide Area Network)

Figure 26: Use Case Energy consumption management

12.4.2.5 Energy Consumption Management - Home Customer

Home customers can have their energy consumption measured, monitored, and their energy consumption and home appliances controlled remotely. For example, the time of running a washing machine could be set to later in the day to avoid electricity consumption during peak times. This can be done by the energy management company, the utility, or the energy retailer, which will establish an agreement with the end-user. In some cases, the home energy management gateway could be co-located with a smart meter, sharing the same communication link.

The role of the MNO in this case is to provide the communication between the end-user smart meters and home energy management system in the home and the service provider. The MNO could also be providing a local or neighbourhood network communication. Additionally, the MNO could play the role of the energy management company.

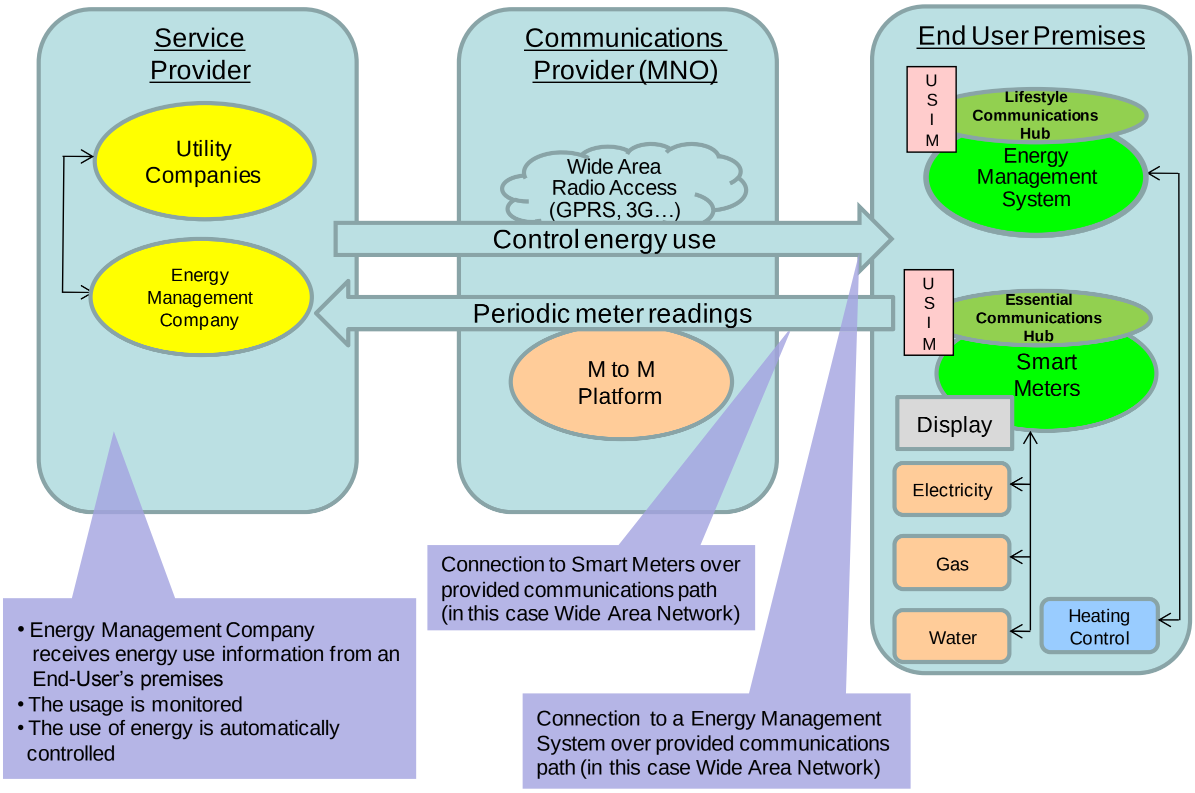

Service Provider
Utility Companies
Energy Management Company
Communications Provider (MNO)
Wide Area Radio Access (GPRS, 3G…)
Control energy use
Periodic meter readings
M to M Platform
End User Premises
USIM
Lifestyle Communications Hub
Energy Management System
USIM
Essential Communications Hub
Smart Meters
Display
Electricity
Gas
Water
Heating Control
• Energy Management Company receives energy use information from an End-User's premises
• The usage is monitored
• The use of energy is automatically controlled
Connection to Smart Meters over provided communications path (in this case Wide Area Network)
Connection to a Energy Management System over provided communications path (in this case Wide Area Network)

Figure 27: Use Case Energy consumption management (Consumer)

12.4.3 Representative Use Cases for the Smart Home sector

This section describes the use cases for the smart home, supported through the embedded mobile home energy gateway.

The use cases that describe core/primary utilities services and end-user control services in the table below might require the home energy gateway to request and send data from and to the smart meter. In these scenarios, there will be an overlap between the use cases provided below and the smart metering use cases described in section 12.4.2.

No.	Use case clusters	Description
1	Core/primary utilities services: 1.1. Information	1.1.1 Current consumption: Provision of information to customers on their current consumption of electricity, water and gas, collected from smart meters, as well as smart home appliances and smart devices. Home owners access an information portal, associated with their home gateway, to view current consumption and status information for a variety of home appliances that are connected to the gateway. The information portal may be accessible via an interface on the home gateway or via an alternative device, such as a PC, tablet or smartphone. 1.1.2 Historical and statistical information on usage and costs. Homeowners are able to retrieve and view historical consumption data for one or more metered utility services. This data includes consumption amounts, as well as charges associated with all services that are linked to the home gateway. 1.1.3 Tariff information for prepaid and post-paid plans: In this use case, home owners can request information about tariffs for different connected utility services that are linked to their home gateway. Tariffs specific to a locality and the incumbent provider may be obtained by

No.	Use case clusters	Description
		the user specifying a location or by the gateway automatically indicating its location. 1.1.4 Market information around prices for utilities services, and information on the incentives for energy efficiency. In this use case, home owners may search for and request tariff information from multiple providers and in each utility segment for their neighbourhood. Homeowners can also request information from consumer-advocacy and local government agencies about energy efficiency incentives. Both classes of information request may be enabled directly via the home gateway user interface or a linked PC/tablet/smartphone device.
	1.2. End-User Control	1.2.1. Remote control of home appliances. Home owners can program their home gateway to control each of the connected devices associated with the gateway. Control functions may be implemented through pre-set rules (time-of-day, threshold or alarm driven etc.). They may also be implemented using remotely-issued commands delivered via a SMS message, for example, from the homeowner to change the home temperature setting, possibly overriding an existing control rule. 1.2.2. Prepayment for utilities services. In this use case, the home gateway functions as a pre-paid controller for individual utility services. In the case of electricity, for example, the home owner may have credited the household account. The gateway monitors on-going consumption, sends alerts when certain thresholds are reached and then suspends electricity supply when the credit amount has been exhausted. The gateway user interface may allow the credit level to be topped-up directly. It may also include an emergency indicator to allow a certain level of over-consumption according to criteria set by the utility provider based on the homeowner's credit history.
	1.3. Utility Control	1.3.1. Demand response. For a homeowner who has enrolled in a demand response programme, the home gateway responds to control signals from the utility company to curtail the power being consumed by the household. Control is exerted over devices such as HVAC (heating, ventilation, air-conditioning), lights, pool pumps, appliances, etc. that are connected to the home gateway. In some situations, demand response may be used to encourage consumption, or local storage, when the average load on the grid is sub-optimally low. 1.3.2. Load curtailment inquiry. This use case is similar to demand response. Homeowners are offered financial incentives to reduce their energy use when the utility provider determines it is needed. When the homeowner receives an advance notice of a price that is to their advantage, they can then pledge an energy reduction. The homeowner then takes steps to reduce his consumption, using the rule-based functions in the gateway, for example. Usage data is monitored via the home gateway to calculate the potential and actual reduction in use and to provide the information for any payment settlement. 1.3.3. Mobile provider switching. In this use case, a utility provider supplies the home gateway to its customers. The gateway is provided in a form where it has been provisioned on a particular mobile operator's network. At a later point in time, the utility can switch to a different mobile operator through a physical replacement of the card or through a remote switching command that implements the switching functionality in an embedded SIM. Other mechanisms for remote switching include roaming SIM/UICC, and the use of multiple UICCs on board. 1.3.4. Application, policy or configuration update. The utility provider uses an over-the-air command to modify or update applications, policies or

No.	Use case clusters	Description
		configuration parameters in the home gateway. This functionality can be applied to the gateway itself and to suitably-configured connected devices linked to the gateway.
2	2.1 In-home energy production	2.1.1. Information for utilities. Homeowners with local electricity generation capabilities that are configured for feed-in to the grid will have this information monitored by the home gateway. The collection of this information, suitably protected by anti-fraud safeguards, is fed back to the utility for its accounting purposes. 2.1.2. Payment/settlement information for utilities. Payment or settlement information relating to a homeowner's consumption and feed-in to the grid is made available via the home gateway or via the interface of a related device. 2.1.3. Control of distributed renewable energy sources (solar, EV, wind) to manage network load. This use case is similar to the demand response use case, but it focuses on control over sources of renewable energy to manage feed-in loads and also to facilitate frequency regulation. 2.1.4. Control of distributed renewable energy sources in response to real-time prices. This use case is similar to load curtailment, but deals specifically with sources of renewable energy. 2.1.5. Emergency use case: Information about solar panels provided to third parties, such as fire-fighters in case of fire, to implement emergency shut-down. The home gateway in this scenario has an emergency mode of operation whereby key information relating to connected devices in the household can be made available to the emergency services in the case of a fire, for example. Key information may be relayed back to the utility provider or a specially-designated emergency services address based on local alarms (e.g. triggering of a fire alarm or home security alarm).
3	3.1. Electric vehicle services	3.1.1. EV charging infrastructure - EV charge control by EV owners. Households with an in-home charging station for an electric vehicle can have this charging station linked to the home gateway. This centralises the monitoring of usage information and control, in the case of demand management type applications. 3.1.2. EV charging infrastructure - Payment/settlement information for end-users. In this use case the home gateway and user interfaces handle payment and settlement information for electric vehicle charging. The configuration of this capability can be more or less sophisticated depending on the quality of the home gateway. In complex scenarios, for example, the set-up should permit different accounts to be handled if the household has more than one car and if the household charging station is used by a visiting car. 3.1.3. EV charging control by utility. This use case is similar to the demand response use case, with the home gateway providing control over equipment related to electric vehicle charging.
4	4.1. Assisted Living services	4.1.1. Assisted living is one class of health applications that may involve the use of connected devices in the home. For more complex applications, the home gateway may act as an information aggregation point for multiple devices and sensors; this may be possible because of the on-board processing and data security capabilities in the gateway. The gateway could also permit information from multiple manufacturer sensors to be combined in order to deliver more complex or higher value services.

No.	Use case clusters	Description
5	5.1. Security services	5.1.1. Remote monitoring of home security devices. In this use case, the home gateway forms a part of the home security system. It integrates inputs for different connected sensors, provides a user interface for configuration commands and includes a secure link (for example, fall-back modes to maximise the success rate in reporting alarms) to report any security-related incidents. 5.1.2. Automated control of home security devices. The home gateway, which forms a part of the home security system, provides a user interface and also hosts applications related to the configuration of the home security system.
6	6.1. Third party services	6.1.1. Third party access to the information on home smart devices. Smart devices in the home are likely be supplied by several different manufacturers. In this use case, the home gateway acts as an aggregation point for home area connectivity to different smart home devices, and provides access to the information about these devices to their manufacturers. This may be for the purpose of remote status monitoring and diagnostics as well as higher level applications. 6.1.2. Third party access to the home gateway to manage home smart devices via an energy management system. This use case variant allows the home gateway to have energy management control over smart devices from different manufacturers. This depends on standards for interoperability, as well as an agreed protocol to implement management and control functions over in-home devices. 6.1.3. A single home gateway for devices connected/serviced by different MNOs (e.g. MNO A for energy management, MNO B for security services). In this use case, the home gateway is capable of being partitioned or shared for the purpose of supporting services provisioned on multiple different mobile operator networks. An example of this could involve smart utility services supported on one operator network and electric vehicle services supported on a second operator's network. The service provider on each network must have full control over its connected devices. In the case of very similar applications, such as household energy and electric vehicles, for example, the gateway needs to facilitate cooperation across the multiple applications.

Table 13: Smart Home Use Cases

12.4.4 Embedded Module Requirements and Solution Design Considerations

The following operating environment conditions apply to the capabilities and feature set of embedded modules and any associated off-module components that are designed for host devices in the smart metering sector:

- Long delivery period / product availability
- Ability to remotely upgrade firmware and software on the smart meter and diagnose faults
- Ruggedness and reliability, to withstand wide changes in temperature and environmental conditions

The following solution design considerations apply to the Home energy gateway devices:

- Hardware/interface considerations: A home energy gateway needs to support connectivity for a variety of devices in the home to the back-end systems of utilities companies, home energy management, home automation and security service providers, as well as, potentially, healthcare companies providing assisted living services. A home energy gateway needs to provide device drivers for physical device interfaces, including broadband technologies, such as Mobile Broadband (2G/3G/LTE), Ethernet and DSL, and interfaces for home area network technologies, such as HomePlug AV/GP, IEEE802.11, USB, ZigBee, Wireless Mbus, G.hn, G,hnem and Bluetooth.
- Communication considerations: In order to support such applications as demand response, home alarm and security, the home energy gateway needs to be always-on, with sleep and stand-by modes available for energy efficiency. Aggregation of non time critical data by the gateway, and off-peak upload of data by the gateway, increase the likelihood of successful delivery.
- Software and application requirements:
  - The home energy gateway software needs to have well-defined interfaces to integrate with the underlying hardware and use well-defined and documented APIs for application development. Usage of common APIs allows a number of applications to directly access the embedded module at the same time.
  - Use IP communication between the gateway and remote servers, as well as with the home automation devices. The use of IPv6 is encouraged (for example, use of IPv6 will be necessary to support the use of SEP 2.0), although backward compatibility might be necessary for the installed base of devices that use IPv4.
- Security considerations: The home energy gateway needs to reassure both end-users and third party service providers that their data is fully secure. It needs to be part of an end-to-end security system, providing secure and automated capture of data from home sensors and devices, storage of this data and its transfer to remote servers. The gateway should support appropriate authentication and privacy control mechanisms (e.g. strong two-way authentication, message authentication and integrity, such as using HMAC), and be capable of providing firewall and virus protection.
- Interoperability: A home energy gateway needs to be interoperable with other end-point devices in the home, as well as the “regulated” energy management gateway and smart meters.

13 Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	13/02/2010	First Draft	Strategy Committee	Svetlana Grant, GSMA
1.0	17/03/2010	Submitted for EMC approval as non-confidential whitepaper	Executive Management Committee	Svetlana Grant, GSMA
2.0	08/03/2011	Release 2 approved		Ton Brand GSMA
3.0	28/03/2012	Release 3 approved		David Maxwell, GSMA

Other Information

Type	Description
Document Owner	GSMA Connected Living Programme
Editor / Company	David Maxwell, 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@gsm.org

Your comments or suggestions & questions are always welcome.

14 References

Ref	Title
[1]	GSMA. TS.06 "IMEI Allocation and Approval Guidelines" version 6.0. [Online] July 2011. http://www.gsma.com/documents/ts-06-6-0-imei-allocation-and-approval-guidelines/20164
[2]	GSMA, "Functional Description of Central Equipment Identity Register", v3.1, Dec 2003
[3]	GSMA Security Group, "Threat Analysis of the GSM System", SG.07, GSMA
[4]	F. Cohen, "Computer viruses: theory and experiments," Computers and Security, vol. 6, pp. 22–35, 1987.
[5]	OMTP Forum, "OMTP Trusted Environment", March 2006, http://www.omtp.org/docs/OMTP_Trusted_Environment_OMTP_TR0_v1_2.pdf
[6]	Intel Low Pin Count (LPC) interface specification, Revision 1.1, August 2002 http://www.intel.com/design/chipsets/industry/25128901.pdf
[7]	UICC-terminal interface; Physical and logical characteristics, 3GPP TS 31.101
[8]	3GPP TS 27.007, "AT command set for User Equipment (UE)".
[9]	ISO 7816-3 Smart Card Standard: Part 3: Electronic Signals and Transmission Protocols
[10]	3GPP TS 11.11: "Mobile Equipment (SIM - ME) interface."
[11]	3GPP TS 31.102: "Universal Subscriber Identity Module (USIM) application"
[12]	IETF RFC 3748: "Extensible Authentication Protocol (EAP)".
[13]	Wireless Local Area Network (WLAN) interworking security, 3GPP TS 33.234
[14]	IETF RFC 4186: "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)"
[15]	IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)"
[16]	ETSI TS 102 310: "Extensible Authentication Protocol support in the UICC"
[17]	Open Mobile Alliance, "Firmware Update Management Object Architecture", OMA-AD-FUMO-V1_0-20070118-C, Jan. 2007
[18]	Open Mobile Alliance, "PEEM Policy Expression Language Technical Specification", OMA-TS-PEEM_PEL-V1_0-20060501-D, May 2006.
[19]	Open Mobile Alliance, "Diagnostics and Monitoring (DiagMon) Management Object", V1.1, http://www.openmobilealliance.org/Technical/release_program/diagmon_V1_1.aspx
[20]	Open Mobile Alliance, OMA Secure User Plane Location V2.0, http://www.openmobilealliance.org/technical/release_program/supl_v2_0.aspx
[21]	Open Mobile Alliance, "OMA Device Management Bootstrap", OMA-TS-DM_Bootstrap-V1_2-20070112-C, Candidate Version 1.2 – 12 Jan 2007
[22]	3GPP TS 23.048: "Security mechanisms for the (U)SIM application toolkit", June 2005.
[23]	Open Mobile Alliance, "Provisioning Smart Card", OMA-WAP-ProvSC-V1_1-20040428-C, 2004.
[24]	OMA, "Smartcard-Web-Server", OMA-TS-Smartcard_Web_Server-V1_0-20070209-C, Candidate Version 1.0 – 09 Feb 2007
[25]	ITU-T Rec. X.693, "ASN.1 encoding rules: XML Encoding Rules (XER)", Dec. 2001
[26]	ETSI, "UICC-Terminal interface; Characteristics of the USB interface (Release 7)", TS 102 600, 30 June 2009
[27]	ETSI 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 8)"
[28]	ETSI, "Smart Cards; Machine to Machine UICC; Physical and logical characteristics (Release 9)", TS 102 671, April 2010

[29]	TS 102 225 Rel-6: “Secured packet structure for UICC based applications”.
[30]	TS 102 226 Rel-6: “Remote APDU structure for UICC based applications”.
[31]	TS 22.115 “Service aspects; Charging and billing”
[32]	3GPP TS 31.115: “Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications”.
[33]	3GPP TS 31.116: “Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications”.
[34]	FCC approvals can be obtained via the FCC website at http://www.fcc.gov/oet/
[35]	ETSI TS 102.689: “Machine to Machine Communications (M2M); M2M service requirements”.
[36]	ETSI TS 102.690: “Machine to Machine Communications (M2M); M2M functional architecture”.
[37]	ETSI TR 102.691: “Machine to Machine Communications (M2M); Smart Metering Use Cases”.
[38]	ETSI TS 102.671, “Smart Cards; Physical and logical characteristics of the M2M UICC”
[39]	ETSI TS 102.484 “Secure channel between the UICC and an endpoint terminal”
[40]	3GPP TS 22.016: “International Mobile Equipment Identities (IMEI)”
[41]	3GPP TS 26.267 v8.2.0: “eCall data transfer; In-band modem solution; General description”.
[42]	3GPP TS 26.268: “eCall data transfer; In-band modem solution; ANSI-C reference code”.
[43]	3GPP TS 22.135: “Multicall; Service description; Stage 1”.
[44]	3GPP TS 23.271: “Functional stage 2 description of Location Services (LCS)”.
[45]	3GPP TS 25.305: “Stage 2 functional specification of User Equipment (UE) positioning in UTRAN”.
[46]	3GPP TR 25.914: “Measurements of radio performances for UMTS terminals in speech mode”.
[47]	AEC - Q100 Rev – G: “Stress Qualification For Integrated Circuits”. http://www.aecouncil.com/AECDocuments.html
[48]	THE ISO/TS (Technical Specification) 16949: common automotive quality system requirements catalogue.
[49]	VDA 2C (German Association of the Automotive Industry) hands-free specifications and audio performance requirements
[50]	3GPP TS 23.060 “General Packet Radio Service (GPRS); Service description; Stage 2“ Release 10
[51]	3GPP TS 24.368 “Non-Access Stratum (NAS) configuration Management Object (MO)”
[52]	3GPP TS 22.368 “Service requirements for Machine-Type Communications (MTC); Stage 1”
[53]	3GPP TS 24.008 “Mobile radio interface Layer 3 specification; Core network protocols; Stage 3”
[54]	ITU-T E.164 “List of ITU-T Recommendation E.164 Assigned Country Codes”
[55]	3GPP TR 22.967 “Transferring of Emergency Call Data”
[56]	European Conference of Postal and Telecommunications Administrations (CEPT), Numbering and Addressing In Machine-To-Machine (M2M) Communications, ECC Report 153, November 2010
[57]	CTIA, Test Plan for Mobile Station Over the Air Performance, Revision 3.1, January 2011

14.1 Smart Home Standardisation Document References

Ref	Document Number	Title
[58]	ISO/IEC 15045	Residential Gateway, Part 1: A Residential gateway model for HES Part 2: Modularity and Protocol
[59]	ISO/IEC 18012	Home Electronic System – Guidelines for Interoperability
[60]	ISO/IEC 29104	Home Electronic System – Residential gateway, Part 2: Modularity and protocol (JTC 1/SC 25 N 1733) – to be finalised on 31-12-2011
[61]	ETSI TS 102 689	ETSI M2M Service Requirements
[62]	ETSI TS 102 690	ETSI M2M Functional Architecture
[63]	HGI-RWD017-R3	Home Gateway Initiative – Requirements for Home Energy Management and Control Service
[64]	HGI-RD008-R3	Requirements for Software Execution Environment
[65]	CENELEC/CEN - EN 50090	Home and Building Electronic Systems (HBES, KNX) prTS 50090-6-4: Residential gateway model for a home and building
[66]	CENELEC/CEN - EN 50491 series	General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS).
[67]	GSMA white paper	Embedded Mobile Guidelines – Release 2, March 2011
[68]	IEEE P1901-2010	IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications
[69]	ITU G.9660	G.hn: Unified high-speed wire-line based home networking transceivers - System architecture and physical layer specification
[70]	ITU G.9661	G.hn Unified high-speed wire-line based home networking transceivers - Data link layer specification
[71]	ITU G.9955 (draft)	G.hnem: Narrow-band OFDM power line communication transceivers - Physical layer specification
[72]	ITU G.9956 (draft)	G.hnem: Narrow-band OFDM power line communication transceivers – Data link layer specification
[73]	IEEE P2030	Smart Grid Interoperability of Energy Technology and Information Technology Operation
[74]	TR-069	CPE WAN Management Protocol, Issue 1 Amendment 3. Broadband Forum, November 2010.

15 List of Acronyms

Term	Description
3GPP	Third Generation Partnership Project
A-GPS	Assisted Global Positioning System
AAI	Analogue Audio Interface
ADC	Analogue-to-Digital Converter
AMR	Adaptive Multi Rate
AP	Application Processor
APDU	Application Protocol Data Unit
API	Application Programming Interface
APN	Access Point Name
ARPU	Average Revenue per User
AVC	Advanced Video Coding
B2B2C	Business to Business to Customer
BARG	Billing, Accounting and Roaming Group (GSMA)
BGA	Ball Grid Array
CCTV	Closed Circuit Television
CDMA	Code Division Multiple Access
CE	Consumer Electronics
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization)
CPU	Central Processing Unit
CS	Circuit Switched
CTIA	Cellular Telecommunications and Internet Association
DCE – DTE	Data Communication Equipment - Data Terminal Equipment
DSL	Digital Subscriber Line
DTM	Dual Transfer Mode
E-UTRAN	Evolved Universal Mobile Telecommunications System Terrestrial Radio Access Network
EAB	Extended Access Barring
EAP-SIM	Extensible Authentication Protocol method for GSM Subscriber Identity Modules
EAP-AKA	Extensible Authentication Protocol - Authentication and Key Agreement
EDGE	Enhanced Data rates for Global Evolution
EDT	Embedded Device Testing
EGPRS	Enhanced General Packet Radio Service
HER	Electronic Health Records
HMAC	Hashed Message Authentication Code
ETSI	European Telecommunications Standards Institute
EV	Electric Vehicle

FCC	Federal Communications Commission
FDA	US Food and Drug Administration
FOTA	Firmware Over the Air
GCF	Global Certification Forum is a working forum consisting of Mobile service providers, test labs, test equipment vendors and device vendors; it is responsible for monitoring and administering test and certification procedures and test plans. The GCF maintains an independent certification scheme for mobile phones and wireless devices that are based on 3GPP standards.
GERAN	GSM/Edge Radio Access Network
GPIO	General-Purpose Input / Output
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global Standard for Mobile Communications
HAN	Home Area Network
HL7	Health Level 7 (formatting and protocol standard)
HLR	Home Location Register
HPMN	Home Public Mobile Network
HSS	Home Subscriber Server
HS[U/D]PA	High Speed [Uplink / Downlink] Packet Access
I2C	Inter-Integrated Circuit
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
I/O	Input/output
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
LAP	Low Access Priority
LBS	Location Based Services
LGA	Land Grid Array
LTE	Long Term Evolution
M2M	Machine-to-Machine
MHRA	Medicines and Healthcare Products Regulatory Agency
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MRD	Mobile Receive Diversity
MSISDN	Mobile Station International Subscriber Directory Number
NMO-I	Network Mode of Operation I
NRE	Non-recurring engineering (costs)
OEM	Original Equipment Manufacturer
OFDMA	Orthogonal Frequency-Division Multiple Access

OS	Operating System
OTA	Over the Air
PAYD	Pay As You Drive
PCI-SIG	Peripheral Component Interconnect Special Interest Group
PCM	Pulse Code Modulation
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PLU	Periodic Locations Area Update
POSIX	Portable Operating System Interface for Unix (application programming interface)
PRU	Periodic Routing Area Update
PS	Packet Switched
PTCRB	PCS-1900 Type Certification Review Board. North American operators' certification body for GERAN, UTRAN and E-UTRAN devices.
PTU	Periodic Tracking Area Update
PWM	Pulse Width Modulation
QoS	Quality of Service
R&TTE	Radio and Telecommunication Terminal Equipment
RHCP	Right Hand Circular Polarization
RF	Radio Frequency
RTOS	Real-Time Operating System
SAMT	Stand-Alone Module Testing
SAR	Specific Absorption Rate
SDIO	Secure Digital Input / Output
SDK	Software Development Kit
SGSN	Serving Gateway Support Node
SMS	Short Message Service
SMT	Surface Mount Technology
SMT	Stand-Alone Module Testing
SPI	Serial Peripheral Interface
SSL	Secure Sockets Layer
SVT	Stolen Vehicle Tracking
TCO	Total Cost of Ownership
TCP/IP	Transport Control Protocol / Internet Protocol
TCU	Telematics Control Unit
TIA	Telecommunications Industry Association
TIS	Total Isotropic Sensitivity
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TRP	Total Radiated Power
SIM	Subscriber Identity Module
SKU	Stock Keeping Unit
UART	Universal Asynchronous Receiver/Transmitter

UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
USB	Universal Serial Bus
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visited Location Register
VPMN	Visited Public Mobile Network
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
(W)WAN	(Wireless) Wide Area Network

Annex 1 Automotive Use Cases

USE CASE	Safety, security and other vehicle services – Breakdown Services (bCall)

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
In its simplest form, a bCall (breakdown call) service will send the current vehicle position to a roadside assistance organization and initiate a voice call. The bCall trigger is usually a switch which must be pushed by the user in order to activate the service. An 'enhanced' bCall service is one where current vehicle diagnostic information is transmitted in addition to the vehicle position. This could, in principle, allow the fault to be diagnosed remotely and appropriate action taken. The enhanced bCall service could also allow the car manufacturer or service centre to remotely lock or unlock the car on request of the car owner.	**Equipment vendor**	Car manufacturer specifies the communications module and integrates it with other on-board electronics.
	System Integrator	May be the car company (vendor) .
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third party service provider.
	Reg/Cert Body	Not applicable

Bearer Requirement	Voice, Low data volume (Position Data and Fault Code Information)
Traffic Pattern	Intermittent, at request
Business Model	Automotive OEM or 3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on traffic charges
Service/QoS Requirement	n/a –ubiquitous coverage desirable
Roaming requirement	Most bCall services are likely to be deployed in vehicles that remain within home network coverage most of the time and only require occasional roaming (for example family car travelling abroad for holiday 1-2 times per year). However, to

	support vehicles sold (or re-sold) for use in a country other than that of manufacture or initial deployment, it should be assumed that many bCall services will also operate in a persistent or permanent roaming context.	
Charging Principles **Home network:** **Roaming (wholesale & retail):**	Home network (MNO) provides billing to service provider	
Regulatory Considerations	Not applicable	
Static or Mobile (why GSM)	Mobility requirement	
Scale of Deployment	**High**	
Expected Life of Deployment	**< 5 years**	

USE CASE LABEL	Safety, security and other vehicle services – Stolen Vehicle Tracking

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
The purpose of a Stolen Vehicle Tracking (SVT) system is to facilitate the recovery of the vehicle after theft. Usually, the owner must first report the theft to the police (obtaining a crime report number) prior to contacting their SVT service provider The SVT service provider will request location data from the TCU in the vehicle periodically and liaise with the police. In some countries there are special requirements from insurers and the police covering the system specification and the robustness of the service provider In more advanced systems, the TCU location will be protected against attack. The TCU may also be capable of sending out automatic theft alerts based on vehicle intrusion or illegal movement. The TCU may also be linked to the Engine Management System (EMS) to enable immobilization or speed degradation by remote command	Equipment vendor	Car manufacturer specifies the communications module and integrates it with other on-board electronics or after-market addition
	System Integrator	May be the car company (vendor)
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third-party service provider.
	Reg/Cert Body	Add. Requirements from police and insurance possible

Bearer Requirement	Low data volume (position information and other vehicle status and control information)
Traffic Pattern	Intermittent, at request
Business Model	Automotive OEM or 3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on traffic charges
Service/QoS Requirement	Ubiquitous coverage
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming.
Charging Principles	Home network (MNO) provides billing to service provider

Home network: **Roaming (wholesale & retail):**	
Security/Fraud Considerations	System should protect against tampering and physical attack. Access to remote disabling capability should be limited to highway safety agencies.
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**High**
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	Safety, security and other vehicle services – Remote Diagnostics

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
• Remote diagnostic services can broadly be grouped into the following different implementations: • Maintenance minder – when the vehicle reaches a certain mileage (for example 90% of the manufacturer’s recommended service interval since the previous service), the TCU will send a message to the owner or the owner’s preferred dealership, advising them that the vehicle is due its service • Health check – either on a periodic basis, or triggered by a request from the owner, the TCU compiles the vehicle’s general status, using inbuilt diagnostic reporting functions, and transmits a diagnostic report to the owner, the owner’s preferred dealership, or to the vehicle manufacturer • Fault triggered – when a fault (DTC) is detected with one of the vehicle systems, this triggers the TCU to send the DTC code and any context information (for example snapshot data) to the owner’s preferred dealer, or to the vehicle manufacturer • Enhanced bCall – when a manual breakdown call is initiated by the owner, the TCU sends both position data and DTC status information to the roadside assistance service or the vehicle manufacturer. See Breakdown Services	**Equipment vendor**	Car manufacturer specifies the communications module and integrates it with other on-board electronics
	System Integrator	Might be the car company (vendor)
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third-party service provider.
	Reg/Cert Body	

Bearer Requirement	Low data volume (vehicle status information)
Traffic Pattern	Intermittent, at request
Business Model	Automotive OEM or 3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on traffic charges
Service/QoS Requirement	Ubiquitous coverage desirable
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming

Charging Principles Home network: Roaming (wholesale & retail):	Home network (MNO) provides billing to service provider
Security/Fraud Considerations	Tamper free equipment; UICC should not be accessible
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**High**
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	**Safety, security and other vehicle services – Insurance Services**	
USE CASE DESCRIPTION	**VALUE CHAIN & KEY PARTICIPANT ROLES**	
• Pay-As-You-Drive (PAYD) schemes offer insurers the chance to reduce costs, more accurately reflect actual risk and provide more competitive products to the end-user based on getting feedback from the vehicle as to when, where, how or how far the vehicle is being driven (or a combination of these factors) • The first PAYD insurance schemes were small-scale trials and, where these were successful, they were launched as full-scale policies available to all owners • Insurance companies are starting to address issues such as privacy, business models and service reliability.	**Equipment vendor**	Car manufacturer specifies the communications module and integrates it with other on-board electronics -- almost always after-market
	System Integrator	May be the car company (vendor) Or after-market equipment provider
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third-party service provider (linked to Insurance company)
	Reg/Cert Body	
Bearer Requirement	Low data volume (driving behaviour, vehicle acceleration, braking, velocity and positioning information)	
Traffic Pattern	At start, during and at end of journey.	
Value Proposition	Provide more tailored policies on car insurance to the customer	
Business Model	Automotive OEM or 3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on traffic charges. Insurance company pays a service provider to provide monitoring service, insurance company passes cost on to insured party	

Service/QoS Requirement	n/a
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming
Charging Principles **Home network:** **Roaming (wholesale & retail):**	Home network (MNO) provides billing to service provider
Security/Fraud Considerations	Tamper-free equipment, UICC should not be accessible or interchangeable. SIM identity relates to customer.
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**High**
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	Connected navigation – Traffic reports

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
• The purpose of a traffic report service is to inform the driver of traffic conditions relevant to the area in which they are driving, or a location on their intended route, so that they may alter their route to avoid heavy traffic if necessary • Traffic reports may be delivered to the driver verbally or visually. Where traffic information is given verbally, this may be from an operator in a call centre or by using on-board or off-board text-to-speech conversion software • Where traffic reports are sent as data to the car, this may be accomplished by using cellular networks or FM/HD/satellite radio (for example RDS-TMC) networks • Information may also include weather information.	**Equipment vendor**	Navigation subsystem equipment manufacturer
	System Integrator	Automaker or service provider
	MNO	May provide the connectivity
	Service Provider	Traffic Information Service or 3rd party service provider
	Reg/Cert Body	

Bearer Requirement	Medium data volume
Traffic Pattern	Intermittent, depending on changes in traffic information
Value Proposition	Provide the driver with up-to-date traffic information, also in areas where RDS-TMC is not applicable.
Business Model	3rd part service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on connectivity
Service/QoS Requirement	n/a
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming
Charging Principles Home network: Roaming (wholesale &	Home network (MNO) provides billing to service provider

retail):	
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**Medium**
Expected Life of Deployment	**< 10 years**

<table>
<tr><td><b>USE CASE LABEL</b></td><td colspan="3"><b>Connected navigation – Route planning (send-to-car)</b></td></tr>
<tr><td colspan="2"><b>USE CASE DESCRIPTION</b></td><td colspan="2"><b>VALUE CHAIN & KEY PARTICIPANT ROLES</b></td></tr>
<tr><td colspan="2" rowspan="5">The purpose of this service is to provide the user with a means of planning their forthcoming journey using a PC, and to download the chosen destination to the vehicle
• To access this service, the owner must have access to a PC and must typically be registered (for example user name and password) to use the service. This service may be provided via the vehicle manufacturer’s web portal, or from a route planning website (for example Google Maps)
• Once they are in the vehicle, the user typically has to manually request the destination download into the navigation system</td><td><b>Equipment vendor</b></td><td>Navigation subsystem equipment manufacturer</td></tr>
<tr><td><b>System Integrator</b></td><td>Automaker</td></tr>
<tr><td><b>MNO</b></td><td>provides the connectivity</td></tr>
<tr><td><b>Service Provider</b></td><td>Automotive OEM or 3rd party service provider</td></tr>
<tr><td><b>Reg/Cert Body</b></td><td>n/a</td></tr>
<tr><td><b>Bearer Requirement</b></td><td colspan="3">Medium to high data volume (depending on amounts of information to be downloaded (POI and so on.))</td></tr>
<tr><td><b>Traffic Pattern</b></td><td colspan="3">At start of the journey.</td></tr>
<tr><td><b>Value Proposition</b></td><td colspan="3">Optimal route planning can be done well in advance, adding POIs to the route before departure.</td></tr>
<tr><td><b>Business Model</b></td><td colspan="3">3rd party service provider will charge customer for service and connectivity;
Arrangement between Service provider and MNO on connectivity</td></tr>
<tr><td><b>Service/QoS Requirement</b></td><td colspan="3">n/a</td></tr>
<tr><td><b>Roaming requirement</b></td><td colspan="3">Combination of occasional roaming, and persistent or permanent roaming</td></tr>
<tr><td><b>Charging Principles</b>
<b>Home network:</b>
<b>Roaming (wholesale &</b></td><td colspan="3">Home network operator (MNO)provides billing to service provider</td></tr>
</table>

retail):	
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**Medium**
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	Connected Navigation - Visually-enhanced navigation

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
Typical navigation directions that rely on a driver to recognize and identify street names at turning points can be challenging and distracting. Enhancing driving directions with real-world visual information is more intuitive as this resembles the way human beings naturally navigate routes. This service provides the user navigation directions that are visually enhanced with real-world video or digital images of the route. Tags or arrows can be superimposed on the video or images to make it clear to the motorist where, and in which direction, turns are to be made. The video or images can be provided for the entire route or at important points in the route, for example, destination, turning points, multi-road intersections, traffic circles, unmarked roads, or multi-lane exits or interchanges. The large database required for such visual images cannot be practically stored or kept up-to-date on media storage in the vehicle navigation system. The service requires high-speed connectivity to download the visual enhancements and driving directions. The connectivity also allows the navigation service provider to leverage existing databases of images and video for the service, for example, Google-Earth and Google Street View.	**Equipment vendor**	Navigation subsystem equipment manufacturer or after-market addition.
	System Integrator	May be the car company (vendor).
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third party service provider.
	Reg/Cert Body	n/a

Bearer Requirement	High data volume
Traffic Pattern	At the start, or throughout, the journey. This depends on the amount of data that can be stored in the navigation system and the length of the route. The majority of the data will be transported on the downlink.
Value Proposition	Provides for a more intuitive and user-friendly navigation experience.
Business Model	3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on connectivity
Service/QoS Requirement	Best effort QoS is sufficient for downloading of images and video prior to presentation.

Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming.
Charging Principles **Home network:** **Roaming (wholesale & retail):**	Home network operator (MNO) provides billing to service provider
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**Medium**
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	**Connected Navigation - Augmented reality POIs**

USE CASE DESCRIPTION	**VALUE CHAIN & KEY PARTICIPANT ROLES**	
Augmented reality (AR) technology uses virtual computer-generated imagery to augment elements of a live direct or indirect view of the physical real-world environment. Using this technology, POI information can be directly superimposed onto a view of the real-world surroundings displayed on either a dashboard LCD screen or projected as a Heads-Up Display on the windshield. The in-vehicle system provides location, and potentially orientation, data with the server to obtain the appropriate POI information and metadata to enable accurate presentation superimposed on a real-world view of the environment.	Equipment vendor	Head-unit supplier and/or navigation subsystem equipment manufacturer. After-market addition possible.
	System Integrator	May be the car company (vendor).
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third party service provider.
	Reg/Cert Body	n/a

Bearer Requirement	High data volume and low-latency
Traffic Pattern	Intermittent when the feature is enabled by the motorist.
Value Proposition	Provides for a rich and intuitive multimedia presentation of POI information.
Business Model	3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on connectivity
Service/QoS Requirement	QoS requirement for bursty low-latency delivery of traffic.
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming.

Charging Principles Home network: Roaming (wholesale & retail):	Home network operator (MNO) provides billing to service provider
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**Medium** (more than 5,000)
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	**Infotainment – information provisioning**	
USE CASE DESCRIPTION	**VALUE CHAIN & KEY PARTICIPANT ROLES**	
The purpose of this service is to provide information to driver and passengers, and may include: - Mobile TC - Internet connectivity for web browsing and email - Location-based interactive e-commerce (for example, shopping or restaurant recommendations, user can reserve a table or book cinema tickets) - Other types	**Equipment vendor**	Head-unit supplier
	System Integrator	Automotive OEM
	MNO	Promotes the service and provides the connectivity
	Service Provider	Automotive OEM or 3rd party service provider
	Reg/Cert Body	n/a
Bearer Requirement	High data volume	
Traffic Pattern	At request – high bandwidth requirement, streaming and bursty traffic	
Value Proposition	Service provider may provide tailored information to a in-built web browser	
Business Model	3rd party service provider or MNO will charge customer for service and connectivity; Arrangement between Service provider and MNO on connectivity	
Service/QoS Requirement	n/a	
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming	
Charging Principles **Home network:** **Roaming (wholesale &**	Home network operator (MNO) provides billing to service provider	

retail):	
Security/Fraud Considerations	May need additional security and fraud requirements if ecommerce is supported
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**Medium** (more than 5,000)
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	Infotainment - Voice-activated digital concierge services

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
The service allows the driver to use natural language to make requests from an automated digital concierge server and obtain rich multimedia responses, for example, "Find two movie tickets for Movie X at 3pm within 20 minutes of my current location". The in–vehicle system makes a recording of the driver's speech and transmits this error-free to a voice recognition server over a high-speed packet data connection. Voice processing in the network enables powerful databases and algorithms such as noise filtering, user-independent natural language interpretation, context-based interpretation, multi-language interpretation, and dynamically-updated vocabularies. The response from the digital concierge service can be integrated into a rich multimedia package consisting of audio, images, URLs, and textual information.	Equipment vendor	Car manufacturer specifies the communications module and integrates this with other user interfaces, or after-market addition.
	System Integrator	May be the car company (vendor).
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third party service provider.
	Reg/Cert Body	n/a

Bearer Requirement	High data volume and low-latency
Traffic Pattern	Intermittent when the feature is enabled by the driver, with more traffic on the downlink.
Value Proposition	Provides for an accurate, natural-language interface to digital concierge services and enables rich multimedia responses.
Business Model	3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on connectivity
Service/QoS Requirement	n/a
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming.
Charging Principles	Home network operator (MNO) provides billing to service provider

Home network: **Roaming (wholesale & retail):**	
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**Medium**
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	**Travel and Traffic Assistance - Assisted Traffic Regulation**	
USE CASE DESCRIPTION	**VALUE CHAIN & KEY PARTICIPANT ROLES**	
Certain aspects of traffic regulation measures can be assisted by transmission of static or dynamic non-critical road regulation information to the car. Examples of this service include the transmission and notification about closed roads, dangerous road conditions, highway tolls, speed limits, based on location information, or even a wrong way warning when on one-way roads. It has to be ensured that the car driver only perceives the transmitted data as supplementary information and does not rely on it. Conventional regulation infrastructure such as traffic lights, road signs etc will always take precedence over the supplementary information.	**Equipment vendor**	Car manufacturer specifies the communications module and integrates it with other on-board electronics or after-market addition.
	System Integrator	May be the car company (vendor).
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the traffic regulation authority or a third party service provider.
	Reg/Cert Body	Not applicable
Bearer Requirement	Low latency needed to enable effective communication	
Traffic Pattern	Intermittent, at request	
Business Model	Automotive OEM or 3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider (and/or traffic regulation authority) and MNO on traffic charges.	
Service/QoS Requirement	n/a –ubiquitous coverage desirable	
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming.	
Charging Principles **Home network:** **Roaming (wholesale &**	Home network (MNO) provides billing to service provider	

retail):	
Regulatory Considerations	It will be required to involve authorities to obtain correct and up-to-date traffic regulation data
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**Medium** (more than 5,000)
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	Travel and Traffic Assistance - Access Control / Parking Zone Management		
USE CASE DESCRIPTION		**VALUE CHAIN & KEY PARTICIPANT ROLES**	
Communication infrastructure, combined with stored user or car credentials, could be used to manage access to specific areas, for example company or private grounds. A gate could be opened by transmitting SIM or TCU stored credentials, or by typing a PIN on a keypad in the car. This system could also assign parking spaces in a parking lot or garage, and take care of the billing as well.		**Equipment vendor**	Car manufacturer specifies the communications module and integrates it with other on-board electronics or after-market addition.
		System Integrator	May be the car company (vendor).
		MNO	Promotes the service and provides the connectivity
		Service Provider	This could be a third party service provider, a security company, or local communities managing their public parking space.
		Reg/Cert Body	Not applicable
Bearer Requirement	Medium latency required to enable effective communication		
Traffic Pattern	Intermittent, at request		
Business Model	Automotive OEM or 3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on traffic charges.		
Service/QoS Requirement	n/a – coverage required in service areas		
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming.		

Charging Principles **Home network:** **Roaming (wholesale & retail):**	Home network (MNO) provides billing to service provider
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Could also be static (for example Wi-Fi) but mobile networks are equally suitable
Scale of Deployment	**Medium**
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	Cloud Computing for Automotive Embedded Modules

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
Cloud computing enables processor and information resources in the network to be shared among many devices. In the case of automotive embedded modules, cloud computing provides a number of benefits: new applications can be deployed on network servers without requiring costly upgrades to the embedded modules, and performing computation and storing information in the network instead of in the embedded modules enables the use of lower-cost modules. In order for cloud computing to be practical in the context of automotive modules, there must be a high-bandwidth, low-latency connection between the modules and the network servers, so that the applications can quickly respond to user input and provide the results of network computations.	Equipment vendor	Car manufacturer specifies the communications module and integrates it with other on-board electronics.
	System Integrator	May be the car company (vendor).
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third party service provider.
	Reg/Cert Body	Not applicable

Bearer Requirement	High data volume and low latency in both directions
Traffic Pattern	Intermittent, at request
Business Model	Automotive OEM or 3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider and MNO on traffic charges
Service/QoS Requirement	n/a –ubiquitous coverage desirable
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming.
Charging Principles Home network: Roaming (wholesale & retail):	Home network (MNO) provides billing to service provider

Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement (services must be delivered while vehicle is moving)
Scale of Deployment	**Medium**
Expected Life of Deployment	**< 10 years**

USE CASE LABEL	Electric Vehicle (EV) Communications

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
Electric Vehicle (EV) charging is a key application of the Smart Grid. An embedded communications module in the EV connects the EV to the charging infrastructure. The embedded module enables the EV to locate and reserve a charging station near its current location when its battery level is low, and the user can remotely check the charging status of their EV while it is charging. The WAN connection provided by the embedded module supports authentication and billing, and makes it possible for the EV to be commanded to provide power back to the grid during peak usage periods.	Equipment vendor	Car manufacturer specifies the communications module and integrates it with other on-board electronics.
	System Integrator	May be the car company (vendor).
	MNO	Promotes the service and provides the connectivity
	Service Provider	This could be the car manufacturer or a third party service provider.
	Reg/Cert Body	Not applicable

Bearer Requirement	Low latency needed to enable effective communication
Traffic Pattern	Intermittent, at request
Business Model	Automotive OEM, power company or 3rd party service provider will charge customer for service and connectivity; Arrangement between Service provider (and / or power company) and MNO on traffic charges.
Service/QoS Requirement	n/a –ubiquitous coverage desirable
Roaming requirement	Combination of occasional roaming, and persistent or permanent roaming.
Charging Principles Home network: Roaming (wholesale & retail):	Home network (MNO) provides billing to service provider and/or power company

Security/Fraud Considerations	Depending on mCommerce capabilities that are added to the service
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobility requirement
Scale of Deployment	**Medium**
Expected Life of Deployment	**< 10 years**

Annex 2 Smart Utilities Use Cases

USE CASE	Vehicle charging controlled by Smart Grid	
USE CASE DESCRIPTION	**VALUE CHAIN & KEY PARTICIPANT ROLES**	
The Utility may offer the Customer an Optimized Energy Transfer Program. This offers the customer and utility an opportunity to take advantage of Regulation services and utilize Spinning reserves and other methods to match grid load to demand in a predictable and accountable aspect. Regulation services are used to continuously fine-tune the balance between power generation and demand, in terms of the voltage and the frequency of the grid. In many power markets, this function, called regulation or automatic generation control (AGC), is priced separately from power generation and procured as an ancillary service (another such service is spinning reserves). The grid operator needs to be able to ensure generators ramp output up or down in real time to meet customer reactive power needs, manage customer impact on system voltage, frequency and system losses and ensure that power-factor problems at one customer site do not affect power quality elsewhere in the system. Again, providing regulation services requires electricity generation capacity in excess of demand. Spinning reserves refers to generating capacity that is up and running, and synchronized with the electricity grid (but not contributing power). Spinning reserves generators contribute to grid stability, helping to arrest the decay of system frequency when there is a sudden breakdown or loss of another generator. Again, typically, power plants that can provide fast response to the calls of the grid operator are the most suitable, for example gas turbines. The capacity required to provide spinning reserves can also be seen as an underutilized investment, although essential for managing market risks. Optimized Energy Transfer programs are designed to incentivize customers whom are willing to give the energy provider control over their load. More specifically these programs allow energy providers to reduce or interrupt customer loads during critical grid events. The idea is that the energy provider based on the grid event can actively manage the charging load by either reducing or interrupting it. In either case, the active management will support turn off those who have higher SOC while only reducing the charge rate of those that have lower SOC. Usually, the energy provider offers a vast array of options with programs varying in the quantity of events and length of reduction or interruption periods. These include Regulation Services and taking advantage of Spinning Reserves.	**Utility or Alternative Energy Supplier (AES)**	Enrols customer in Optimized Energy Transfer programs and manages back office systems and communications with EV / EVSE to enable power services such as regulation and spinning reserves.
	Customer	Enrols in Optimized Energy Transfer programs through utility or AES.
	Electric Vehicle (EV) or Electric Vehicle Supply Equipment (EVSE) manufacturer	Integrates ESCI in on-board electronics of EV or EVSE.
	MNO	Provides WWAN connectivity service to utility or AES.
	Charging Station Operator	Provides EVSE for public charging stations. Has a contract with utility or ASE.

	Distribution Network Operator (DNO), Independent System Operator (ISO) or Regional Transmission Organization (RTO)	Generates real-time signal to utility or AES which defines load changes to be implemented by EVs / EVSEs in order to deliver the committed power services.
Bearer Requirement	High Data rates and low latency needed for optimal performance.	
Traffic Pattern	Intermittent	
Value Proposition	Real-time communications enable smart charging of electric vehicles to provide valuable grid services such as regulation and spinning reserves, providing customers with discounted energy rates for fuelling electric cars.	
Business Model	Utility or AES aggregates EV loads enabling customers to participate and benefit from current power market.	
Service/QoS Requirement	3G data rates and low latency needed for participation in ancillary services market as defined by ISO/RTO (<2s from utility/AES to EV/EVSE according to ISO/RTO council [Assessment of Plug-in Electric Vehicle Integration with ISO/RTO Systems; March 2010: http://www.isorto.org/atf/cf/%7B5B4E85C6-7EAC-40A0-8DC3-003829518EBD%7D/IRC_Report_Assessment_of_Plug-in_Electric_Vehicle_Integration_with_ISO-RTO_Systems_03232010.pdf]	
Charging Principles Home network: Roaming (wholesale & retail):	High data rates and low latency needed for optimal performance.	
Security/Fraud Considerations	Although mobile network authentication will be performed, additional authentication, authorization and encryption may be needed to communicate with utility / AES servers.	
Regulatory Considerations	Utility / AES should be approved by local ISO / RTO / DNO to participate in ancillary services market.	
Static or Mobile (why GSM)	Mobile	
Scale of Deployment	Broad	

Expected Life of Deployment	➢ 3 years

USE CASE	Vehicle-to-grid (V2G) electricity demand, distribution and storage managed by Smart Grid	
USE CASE DESCRIPTION	**VALUE CHAIN & KEY PARTICIPANT ROLES**	
An electrical vehicle provides vehicle-to-grid (V2G) services where the Smart Grid performs peak load levelling by instructing the electrical vehicle to throttle its charging rate or provide power back to the grid. This concept also applies to solar and hybrid/fuel cell automobiles. Low latency of 3G is required to enable integration with current energy markets. The concept allows V2G vehicles to provide power to help balance loads by "valley filling" (charging at night when demand is low) and "peak shaving" (sending power back to the grid when demand is high). It can enable utilities new ways to provide regulation services (keeping voltage and frequency stable) and provide spinning reserves (meet sudden demands for power). In future development, it has been proposed that such use of electric vehicles could buffer renewable power sources such as wind power, for example, by storing excess energy produced during windy periods and providing it back to the grid during high load periods, thus effectively stabilizing the intermittency of wind power. Some see this application of vehicle-to-grid technology as a renewable energy approach that can penetrate the baseline electric market. It has been proposed that public utilities would not have to build as many natural gas or coal-fired power plants to meet peak demand or as an insurance policy against blackouts. Since demand can be measured locally by a simple frequency measurement, dynamic load levelling can be provided as needed.	**Utility or Alternative Energy Supplier (AES)**	Utility or Alternative Energy Supplier (AES) specifies the Energy Services Communication Interface (ESCI) to be implemented in Electric Vehicle (EV) or Electric Vehicle Supply Equipment (EVSE). Enrols customer in V2G programs and manages back office systems and communications with EV / EVSE.
	Customer	Enrols in V2G programs through utility or AES.
	EV or EVSE manufacturer	Integrates ESCI in on-board electronics of EV or EVSE (electric vehicle supply equipment).
	MNO	Provides WWAN connectivity service to utility or AES.
	Distribution Network Operator (DNO), Independent System Operator (ISO) or Regional Transmission Organization (RTO)	Generates real-time signal to utility or AES which defines instant load or generation requirements to be implemented by EVs / EVSEs in order to deliver the committed power services.

Bearer Requirement	High data rates
Traffic Pattern	Intermittent
Value Proposition	Real time communications enable EV / EVSE to participate in energy markets, generating value in the form of revenue, energy credits or reduced energy rates for customers.
Business Model	Carbitrage: This is a fusion of 'car' and 'arbitrage'. When the electric utility would like to buy power from the V2G network, it holds an auction. The car owners are able to define the parameters under which they will sell energy from their battery pack. Many factors would be considered when setting minimum sale price including the cost of the secondary fuel in a PHEV and battery cycle wear. When this minimum price is satisfied, it is deemed as meeting carbitrage.
Service/QoS Requirement	3G data rates and low latency needed for participation in ancillary services market as defined by ISO/RTO. Compliance of ESCI with requirements by utility or AES.
Charging Principles **Home network:** **Roaming (wholesale & retail):**	High data rates and low latency needed for optimal performance.
Security/Fraud Considerations	Although mobile network authentication will be performed, additional authentication, authorization and encryption may be needed to communicate with utility / AES servers.
Regulatory Considerations	Utility / AES should be approved by local DNO / ISO / RTO to participate in power market.
Static or Mobile (why GSM)	Mobile – the electrical vehicle may be connected to a charging station anywhere.
Scale of Deployment	Broad
Expected Life of Deployment	➢ 5 years

USE CASE	Ad-supported electric vehicle charging

USE CASE DESCRIPTION	VALUE CHAIN & KEY PARTICIPANT ROLES	
When customer plugs en EV for charging, the vehicle and perhaps the user are authenticated and authorized as part of the service provision. Customized audio & video advertising is delivered by utility or AES through multimedia EVSE stations (public or private). Advanced versions of the system would allow delivery of printed and electronic coupons (for example SMS message with code) or even instant purchases of goods and services.	**Utility or Alternative Energy Supplier (AES)**	Supplies energy to charging station operator for charging EVs.
	Charging Station Operator	Provides energy service to customers for charging EVs, and deliver advertising services using multimedia EVSE infrastructure. Provides EVSE for public charging stations.
	Customer	Enrols in energy supply service with utility or AES, and receives advertising when charging as added service or in exchange of a discounted energy rate.
	MNO	Provides WWAN connectivity service to utility or AES.
	Multimedia company/Advertising company	Provides content to EV customer.
	EVSE manufacturer	Manufactures multimedia EVSE.

Bearer Requirement	High data rates
Traffic Pattern	Intermittent, high throughput and low latency
Value Proposition	Real time, high throughput communications enable EVSE to act as media channel in the benefit of advertisers, service providers (utility or AES) and customers.
Business Model	Service provider (utility or AES) collects revenue from advertisers in order to use multimedia EVSE for advertising purposes. Customers benefit from relevant customized coupons and prospective discounts in energy rates.
Service/QoS Requirement	3G/4G data rates and low latency needed for real-time delivery of advertising material (video, audio, coupons).

Charging Principles Home network: Roaming (wholesale & retail):	High data rates and low latency needed for optimal performance.
Security/Fraud Considerations	Although mobile network authentication will be performed, additional authentication, authorization and encryption may be needed to communicate with utility / AES servers.
Regulatory Considerations	Not applicable
Static or Mobile (why GSM)	Mobile – the electrical vehicle may be connected to a charging station anywhere.
Scale of Deployment	Broad
Expected Life of Deployment	➢ 2 years