eSIM Whitepaper

The what and how of Remote SIM Provisioning

March 2018

Table of Contents

eSIM Whitepaper 1

The what and how of Remote SIM Provisioning 1

Introduction 3

How it Works 4

SIM Cards Today 4

Remote SIM Provisioning 5

The Profile 6

Overview of the M2M Solution 7

Main System Elements 7

SM-DP 7

SM-SR 8

eUICC 8

Compliance 8

Overview of the Consumer Solution 9

Main System Elements 9

SM-DP+ 9

LPA 9

eUICC 10

SM-DS 10

Compliance 10

Why are there two Solutions? 12

Common Features to both solutions 12

Unique features of the M2M solution 13

Unique features of the Consumer Solution 14

Differences in Compliance 15

Compliant Devices and Platforms are Essential 16

Conclusion 17

Annex - Frequently Asked Questions 18

Introduction

The ubiquitous SIM card has played a fundamental role in mobile telecommunications for over 25 years. It is recognised by end users and provides a secure means for authenticating devices onto networks, all inside a removable “Secure Element”, which is easily transferrable between mobile devices.

Although the role of the SIM itself is not changing, the GSMA has defined a radical new way to load it into devices. Now the SIM may be securely downloaded into a ‘Secure Element’ that can be permanently embedded inside any type of device. To enable this change, an ecosystem of trusted platforms and players has been facilitated by the GSMA to create the eSIM solution. It offers an equivalent level of security and protection to that provided by the removable SIM card.

The change from the Removable SIM to an eSIM provides benefits for many players:

- **For *everyone,* eSIM provides an equivalent level of security as the removable SIM card**. This is **vital** as it is the subscription credentials stored on the SIM card that enable secure and private access to mobile networks. It also supports the integrity of the billing process, especially in roaming scenarios:
- **For the device end user,** eSIM enables simplified management of subscriptions and connections. End users will no longer have to manage several SIM cards:
- **For organisations**, eSIM enables remote management of subscriptions. This is a significant benefit where devices are not managed by the end user or are not be readily accessible (for example due to operational scale, making individual device management cost prohibitive). This enables pioneering categories of connected devices:
- **For distributors**, simplified logistics are possible, customisation for specific operators or regions may be reduced:
- **Operators** will have simpler means to expand their businesses into emerging markets, for example, automotive, wearables and consumer electronics. SIM card distribution costs will be eliminated, and eSIMs will enable new distribution models for devices and for marketing of subscriptions:
- **Device Manufacturers**, can exploit the reduced space within their products to make smaller devices. Their products could also be made more tolerant to environmental factors such as dampness, temperature and vibration as they can be hermetically (completely airtight) sealed. Manufacturers can also leverage eSIMs to optimise supply chain processes.

This document provides both a primer to introduce the basics of Remote SIM Provisioning technology and an introduction to the detailed technical specifications.

For more information on GSMA solutions for eSIM (including support material for organisations wishing to deploy eSIM solutions) and enrolment to use the GSMA eSIM logo, please go to https://www.gsma.com/esim/.

How it Works

Conceptually the principle behind eSIM is simple. The integrity of traditional SIM cards is safeguarded by using secure facilities for their manufacture, which includes loading of software and operator credentials. Operator logistics channels then distribute the SIM cards to the required endpoints, for example retail shops, retail partners or enterprise customers managing fleets of connected devices.

eSIM extends the reach of the secure facilities from specific physical locations, to any location where the device can be reached over the internet. eSIM protocols provide security and integrity for data transfer. This, however, is only one part of the challenge. As well as being secure, the distribution channels for SIM cards also contain ‘business logic’ which is required by various service models. In some channels that logic may even dictate who has control of device connections. It is not practical to combine this logic into a single technical solution for eSIM. The GSMA has created solutions suited to different types of channels:

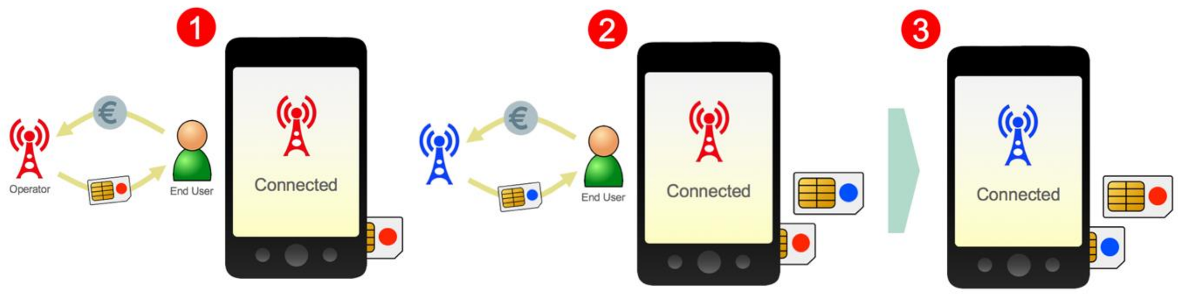
- **Consumer solution**: for the ‘direct to consumer’ channel, this solution is required where the end user (or consumer) has direct choice of the operator supplying connectivity. Consumer solutions require a high degree of end user interaction, with the principle that the end user is familiar with operating the end user interface and actively choosing their network connectivity provider. The Consumer solution also targets enterprises who use devices targeted to the consumer market.
- **M2M solution:** for the ‘business to business to consumer’ channels, this solution serves the needs of business to business customers, specifically in the Internet of Things (IoT) market.

This section explains the technology at a conceptual level. Later sections provide more detail on the specific technologies used for the Consumer and M2M solutions.

For the purpose of this section, the examples given use the consumer model. It should be noted that the M2M model is different in respect that there is no end user interaction as part of profile management and therefore all SIM provisioning operations are managed remotely.

SIM Cards Today

Today, the traditional SIM card is owned and issued by a specific operator. This model is illustrated in the following figure.



SIM Card Operation

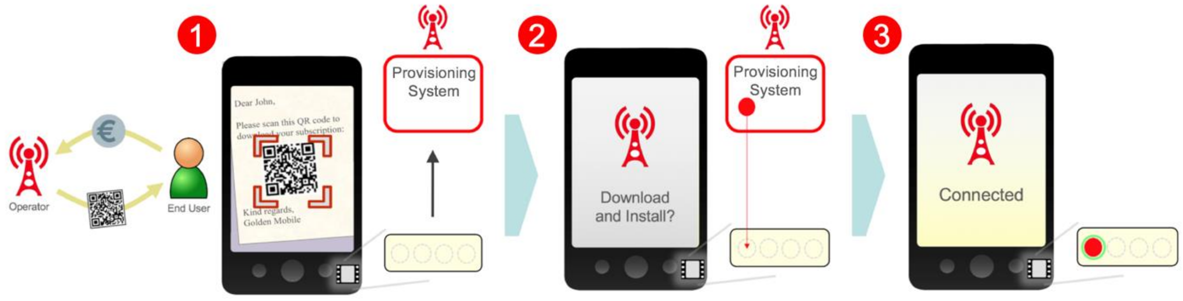
In (1), the end user sets up a contract with their chosen mobile network operator, and in return they receive a SIM card, which they can insert into their mobile device to enable it to connect to the operator's network. This particular SIM card is marked with a red dot to indicate that the subscription credentials contained within it are issued and authenticated by that operator.

Should the end user wish to change operator, they can set up a contract with the new operator (2), and in turn receives a SIM card from that operator (this time marked with a blue dot indicating different subscription credentials).

It is obvious to note that even though the end user has this new SIM card in their possession, the mobile device is still connected to the original operator's network. To change operators, the end user must physically swap the SIMs (3).

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.



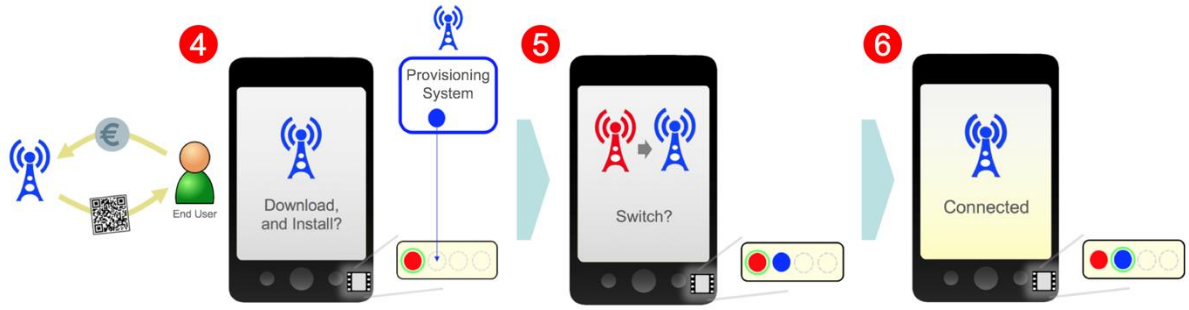
Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.



Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

[3] http://simalliance.org/euicc/euicc-technical-releases/.

Overview of the M2M Solution

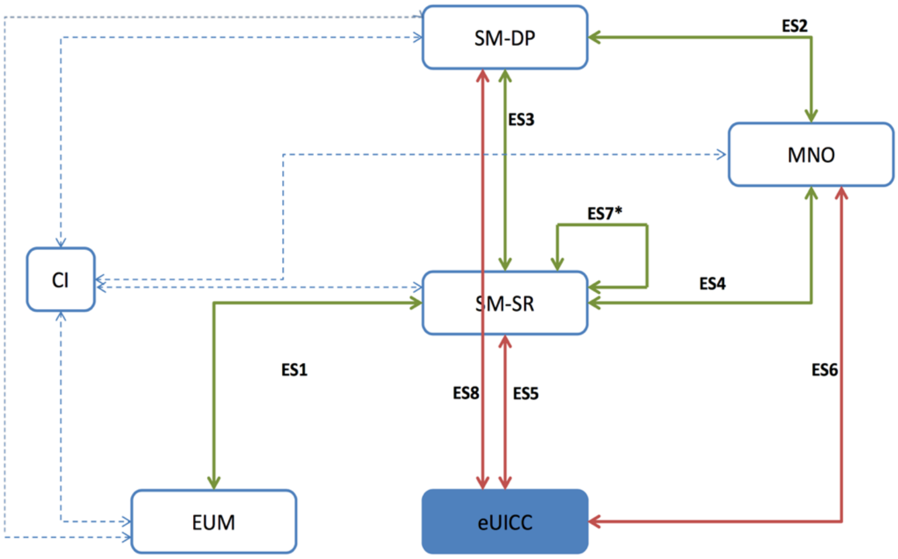
The GSMA M2M solution[4] was the first Remote SIM Provisioning solution developed. There were two reasons for this:

- The M2M solution is simpler as end user interaction is not required, or desirable, in the business to business to consumer (B2B2C) segment, and
- The immediate commercial need was for technical solutions that supported B2B2C deployments alongside regulatory requirements for the launch of services such as eCall[5].

Main System Elements

Remote SIM Provisioning for M2M utilises a server driven (push model) to provision and remotely manage operator Profiles. The solution is organised around 3 elements: the SM-DP (Subscription Manager - Data Preparation), the SM-SR (Subscription Manager - Secure Routing) and the eUICC.

The diagram below is the high-level representation of the M2M main system elements. Beyond common SIM functions, such as SIM Toolkit[6] and Bearer Independent Protocol (BIP[7]) support, the M2M solution does not impose additional requirements on M2M devices to enable usage of eUICCs.



M2M Architecture

SM-DP

The SM-DP is responsible for preparing, storing and protecting operator Profiles (including the operator credentials). It also downloads and install Profiles onto the eUICC.

[4] https://www.gsma.com/iot/embedded-sim/
[5] https://ec.europa.eu/digital-single-market/en/ecall-time-saved-lives-saved
[6] ETSI TS 102 223.
[7] ETSI TS 102 127.

SM-SR

The SM-SR is responsible for managing the status of Profiles on the eUICC (enable, disable, delete)[8]. It also secures the communications link between the eUICC and SM-DP for the delivery of operator Profiles.

eUICC

The eUICC is a secure element that contains one or more subscription Profiles. Each Profile enables the eUICC to function in the same way as a removable SIM issued by the operator that created it. An eUICC may be built using any form factor from the traditional removable card to embedded formats soldered into devices.

Compliance

To reassure all participants that the eSIM ecosystem is secure, a set of criteria[9] that demonstrates compliance to the core requirements has been developed. Compliance with the GSMA M2M specification requires verification of:

- **eUICC Security**, referencing a Common Criteria Protection Profile[10,11] to the assurance level of EAL4+.
- **Production Environment and Process Security**, via the GSMA's Security Accreditation Scheme[12]: SAS-UP (for eUICC personalisation) or SAS-SM (for Subscription Management platforms).
- **Functional Compliance**, based on the GSMA's test specification[13]. GlobalPlatform have created and run a functional test and qualification programme for eUICCs based on the GSMA defined test cases.

Only eUICC manufacturers, and SM-SR and SM-DP hosting organisations that have successfully been accredited by the GSMA SAS can apply for the necessary certificates from the GSMA Certificate Issuer to participate in the GSMA approved ecosystem.

[8] Management of Profile status may be subject to operator business rules.

[9] https://www.gsma.com/iot/embedded-sim/compliance/

[10] https://www.commoncriteriaportal.org/

[11] https://www.gsma.com/newsroom/wp-content/uploads//SGP_05_v1_1.pdf

[12] https://www.gsma.com/sas

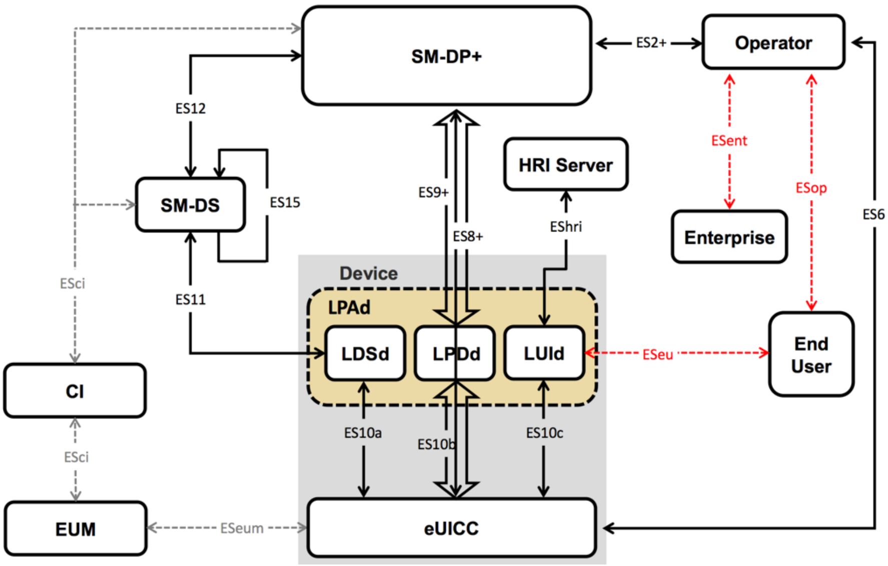
[13] https://www.gsma.com/iot/wp-content/uploads/2014/10/SGP-11-Remote-Provisioning-Architecture-for-Embedded-UICC-Test-Specification.pdf

Overview of the Consumer Solution

The GSMA Consumer solution[14] has been developed from the base provided by the M2M solution, plus consideration of requirements for end user-managed devices. This solution is required to manage use cases are more complex than the M2M solution. Consequentially, more features are required in the specification. In particular the Consumer solution manages end user interaction via the mobile device end user interface, and also supports standalone and companion device types[15].

Main System Elements

The GSMA Remote SIM Provisioning Consumer solution follows a client driven (pull model) and enables control over remote provisioning and local management of operator Profiles by the end user of the device. The solution is organised around 4 elements: the SM-DP+ (Subscription Manager - Data Preparation +), the SM-DS (Subscription Manager - Discovery Server), the LPA (Local Profile Assistant) and the eUICC.



Remote SIM Provisioning for Consumer Architecture

SM-DP+

The SM-DP+ is responsible for the creation, download, remote management[16] (enable, disable, update, delete) and the protection of operator credentials (the Profile). It is given the + designation as it encapsulates the functions of both the SM-DP and the SM-SR of the M2M solution.

LPA

The LPA (Local Profile Assistant) is a set of functions in the device responsible for providing the capability to download encrypted Profiles to the eUICC. It also presents the local management end

[14] https://www.gsma.com/ESIM/
[15] Companion devices are those that rely on a primary device to manage the connections required to install and manage operator Profiles. Such devices are typically wearable IoT type devices such as smart watches.
[16] Remote Management features from version 3 onwards.

user interface to the end user so they canmanage the status of Profiles on the eUICC[17]. The principal functions of the LPA may also be in built into the eUICC.

eUICC

The eUICC in the Consumer solution serves the same high-level purpose as the eUICC in the M2M solution. Implementation is different to support the end user interaction within the Consumer solution.

SM-DS

The SM-DS provides a means for an SM-DP+ to reach the eUICC without having to know which network the device is connected to. This feature is important as devices can be connected using different access networks with different addresses. The SM-DS overcomes this by allowing SM-DP+ to post alerts to a secure noticeboard and for devices to extract those alerts. It is used to notify the LPA when Profile data is available for download to the eUICC. Notifications are sent from the SM-DP+ to the SM-DS. The device LPA polls the SM-DS for notifications when required (supporting the “pull” model). Polling frequency is determined by the eUICC state and by end user actions.

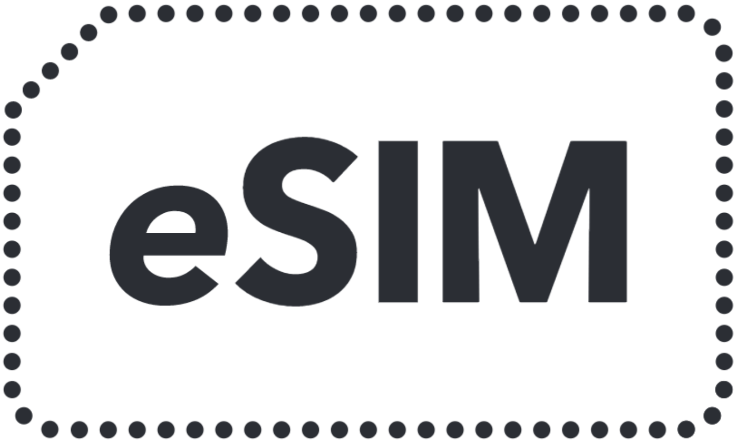
Compliance

Compliance with the GSMA Consumer solution specification[18] requires verification of:

- **eUICC Security**, using the same mechanisms as the M2M specification, although initially focussing only on a silicon-level Protection Profile (PP0084)[19]. A GSMA specified Protection Profile to the level of EAL4+ is currently under development[20].
- **Production Environment and Process Security**, as used in the M2M specification, the GSMA’s Security Accreditation Scheme[21]: SAS-UP or SAS-SM according to the Consumer solution entity type.
- **Functional Compliance**, for all Consumer solution entities, via functional test and certification programmes based on GSMA test specification SGP.23[22]. These programmes have been established, in partnership with GSMA, by GlobalPlatform[23] (for eUICC), Global Certification Forum[24] and PTCRB[25] (for Consumer solution devices).

eUICC manufacturers, and SM-DP+ and SM-DS hosting organisations that have successfully proven their compliance to both the security and functional requirements can apply for the necessary certificates from the GSMA Certificate Issuer to participate in the GSMA approved Consumer solution ecosystem.

[17] Profile management operations may be subject to operator business rules.
[18] https://www.gsma.com/rsp/guide-rsp-compliance-process/
[19] https://www.commoncriteriaportal.org/files/ppfiles/pp0084a_pdf.pdf
[20] GSMA PRD SGP.25
[21] https://www.gsma.com/sas
[22] https://www.gsma.com/newsroom/all-documents/sgp-23-v1-2-rsp-test-specification/
[23] https://www.globalplatform.org/compliance.asp
[24] http://www.globalcertificationforum.org/certification.html
[25] Formerly the PCS Type Certification Review Board, https://www.ptcrb.com/



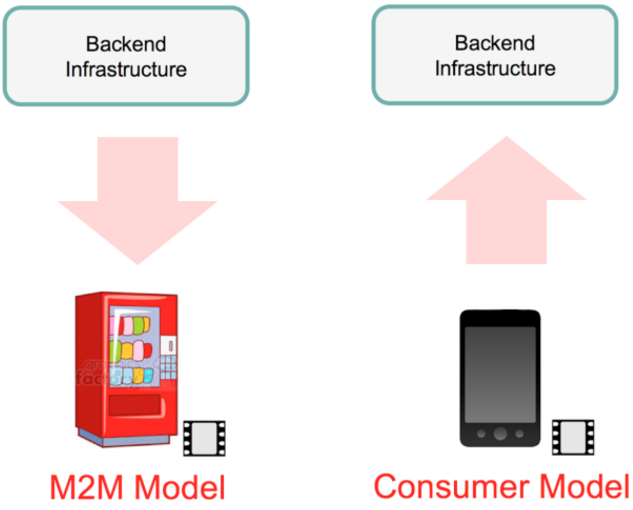
eSIM logo

To assist in the recognition of eSIM capable devices, the GSMA have created a logo that can be used in association with any device that supports eSIM, allowing the user to download operator subscriptions over the air. Use of the logo is freely available to any organisation[26].

[26] Subject to acceptance of the Terms of Use, and the Logo Guidelines.

Why are there two Solutions?

The fundamental difference between the two GSMA Remote SIM Provisioning solutions is the direction of control.



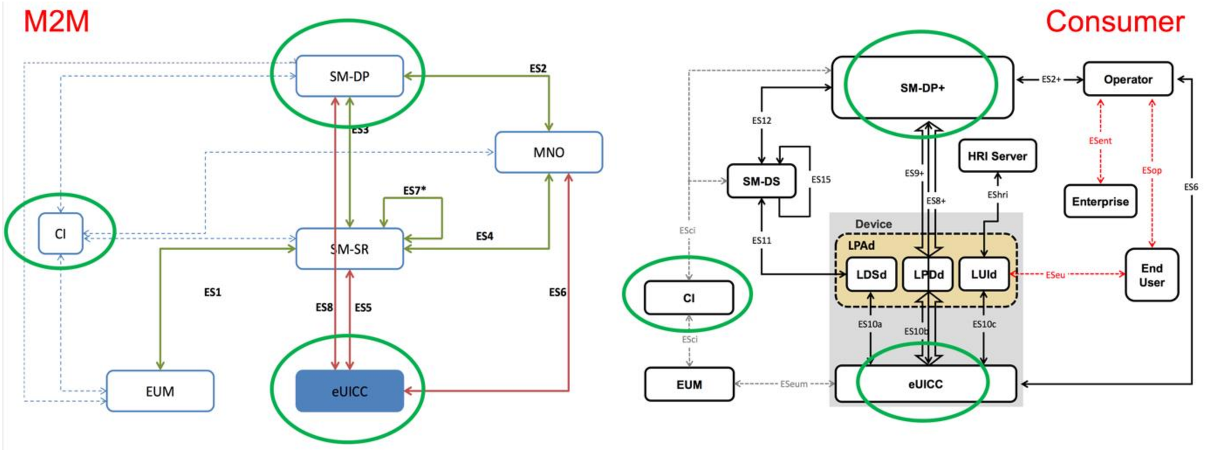
Direction of Control

In the M2M solution, the mobile device normally operates without any local human control of connectivity. This means that it is managed by the operator backend infrastructure, for example, provisioning, billing and their CRM systems. This will select the Profiles to be downloaded and to be enabled/disabled depending, for example, on which country the device is operating in.

By contrast, the Consumer solution requires that all subscription Profile operations are under end user control, or at least subject to end user permission. This is done through an end user interface on the device. For a ‘companion’ device, like a watch, the end user interface may be provided on a ‘primary’ device like a phone or tablet that can provide a more end user-friendly interface for the interactions required.

Common Features to both solutions

The following diagram shows the common features and entities of both specifications.



Common Features

Both architectures feature a network-domain Remote SIM Provisioning system (SM-DP/SM-DP+), but the platform in the Consumer solution(SM-DP+) has extra capabilities, some subsumed from the SM-SR, and others required to support functions specific to the Consumer solution.

Both architectures rely on a secure element within the mobile device for the storage, management and operation of Profiles (eUICC).

Both architectures use Pre-Shared Key (PSK) and Public Key Infrastructure (PKI) based cryptography. However, for the M2M solution authentication with the SM-SR uses PSK and only allows a single SM-SR to communicate with the eUICC. For the Consumer solution, the PKI based authentication is used and therefore any eUICC and SM-DP+ can connect so long as they share the same root PKI certificate.

Both architectures require a GSMA Certificate Issuer (CI) that issues digital certificates which enable entities to securely communicate with each other, and in the Consumer solution, mutually authenticate each other.

It should be noted that although there are architectural similarities between the Consumer and M2M solutions, they are inherently technically different and cannot be overlapped in an implementation that serves both Consumer and M2M.

Unique features of the M2M solution

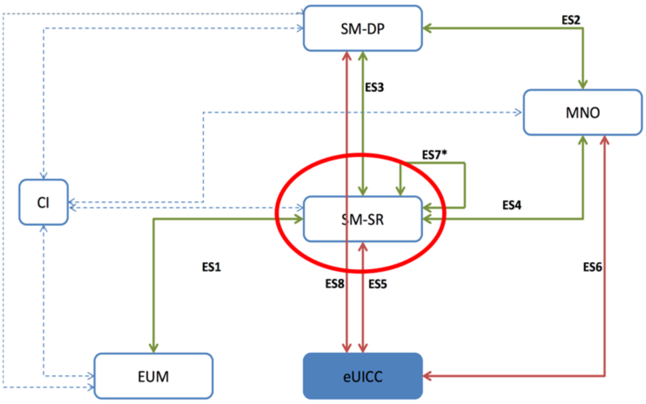
In M2M, everything is remotely managed, requiring no human interaction.

In the M2M solution, the eUICC connects to the SM-SR using Bearer Independent Protocol (BIP)[27], where the underlying bearer being either SMS, CAT_TP[28] or TCP/IP. Bearer choice and termination can have an impact on the performance of the download. Device adaptation is not required for the M2M solution.

[27] However the connection may also use cellular data connections.

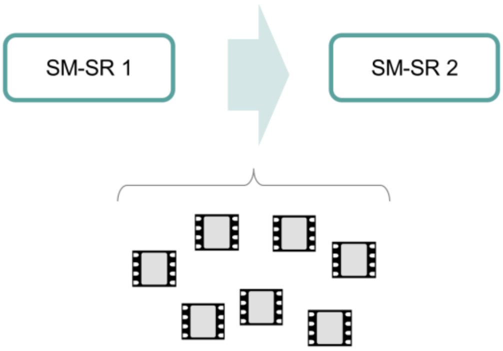
[28] Card Application Toolkit Transport Protocol, ETSI TS 102 127

The M2M solution includes the SM-SR that is not required in the Consumer solution. The SM-SR acts as a gateway from the operator and SM-DP through to the eUICC. The SM-SR holds a database of all the eUICCs under its control and the key sets used to manage them.



Unique features of the M2M solution

A group of deployed eUICCs are managed by a single SM-SR. When there is a change of operator, under some circumstances there may also be a need to move the management of that group of eUICCs to another SM-SR. This SM-SR swap includes transferring the group of eUICCs using a defined SM-SR Swap procedure, and the negotiation of new cryptographic keys with each eUICC received by the new SM-SR.



SM-SR Swap

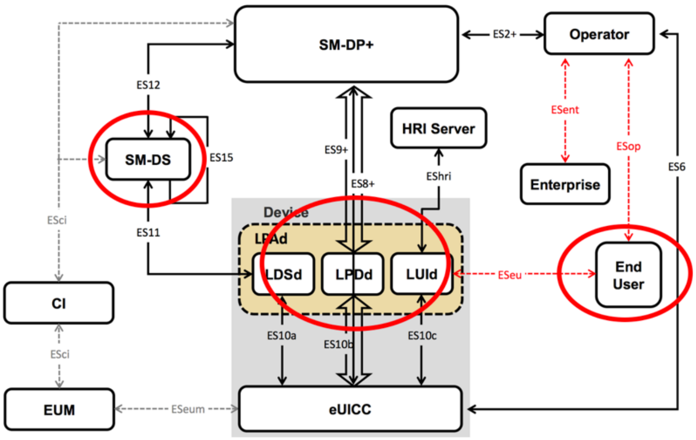
Unique features of the Consumer Solution

In the Consumer solution, the end user manages their own device and Profiles within it.

The Consumer solution has the LPA in the device (or eUICC) that assists with the download of Profiles and secures the end user interface on the device that is used for local control.

All Profile downloads use IP protocols, and where applicable use the greater capacity of the device TCP/IP stack to reduce the communication overhead.

As messages cannot be pushed to the device and eUICC, there is a 'Discovery Service' that devices can check from anywhere, at any time, in order to see if there are any Profiles or management operations waiting to be downloaded from an SM-DP+.



Unique features of the Consumer solution

Differences in Compliance

The principles of compliance are similar for both M2M and the Consumer. The following must be verified:

- Production environment and process security
- eUICC security
- Functional compliance

M2M was set up with clear compliance requirements and a simple process to establish compliance.

Building from the M2M implementation experience, the GSMA enhanced the compliance process for Consumer solutions. This places greater emphasis on functional compliance, which has to be demonstrated before the eUICC manufacturer or Subscription Management platform provider can apply for a digital certificate from the GSMA Certificate Issuer. The compliance process is up and running for all Consumer solution product types, with a similar scheme now being considered for M2M to strengthen the entire ecosystem.

Compliant Devices and Platforms are Essential

During their normal deployment processes, vendors and operators would expect to perform extensive interoperability and compatibility testing. In this case between, for example:

- eUICC and the Subscription Management platforms (for example installed certificates, functional behaviour),
- eUICC and the device (for example the UICC Refresh command support is mandatory for both solutions),
- Device and the Subscription Management platforms (for Consumer solution only, with the LPA),
- Operator Profile and the targeted eUICC.

Therefore, to minimise the need for repetitive interoperability testing, the various stakeholders looking to deploy Remote SIM Provisioning must check that all their suppliers have products satisfying the relevant GSMA product compliance process covering:

- Product certification
- eUICC product security assurance
- Product site and data-centre accreditation according to the GSMA Security Accreditation Scheme (SAS)

And subsequently perform:

- Issuance of certificates by a GSMA Certificate Issuer for compliant products.

Conclusion

The GSMA has created solutions to allow the adoption of eSIM technology to meet the particular needs of both M2M and Consumer markets.

This paper gives an overview of these solutions, and how they meet the various identified market needs.

These solutions will evolve to meet new market needs for eSIM as perceived by the GSMA membership.

For further information, please refer to the GSMA eSIM website at https://www.gsma.com/esim/.

Annex - Frequently Asked Questions

Can a device without a Profile connect to a mobile network?

A device without a Profile loaded and enabled may use a number of alternative methods to download a Profile. These include using a special purpose ‘Provisioning Profile’ to connect to a cellular network for both Consumer and M2M solutions, or for the Consumer solution only there is also the additional options of using a non-cellular network (e.g. Wi-Fi) or a primary device with its own cellular connection.

What is a consumer device?

A ‘consumer device’ is considered to be any device where the consumer, device owner or end user has a direct contract or relationship with an operator of their choice to operate the device.

What is a Companion Device? And a Primary Device?

A Companion Device is a device that relies on the capabilities of a primary device for the purpose of Remote SIM Provisioning. A primary device is a device that can be used to provide capabilities (e.g.: touch screen keyboard, page-sized display) to a companion device for the purpose of Remote SIM Provisioning.

Will the traditional SIM card be phased out?

The use of the traditional SIM will very likely decrease over time based on the availability and penetration of devices supporting Remote SIM Provisioning.

Will Remote SIM Provisioning remove the need for international roaming?

Remote SIM Provisioning will not replace the roaming services provided by operators.

How much memory will be available in an eUICC and how many Profiles can be stored into it?

The memory of an eUICC can range from several KB to several MB. There is no specific limit on the number of Profiles that can be stored on an eUICC, this depends only on memory available and the size of Profiles. Operators could manage Profile sizes to fit them in the eUICC.

What is the ‘GSMA approved ecosystem’?

Both the Consumer and M2M solutions require trusted platforms to interoperate with each other. For both solutions the GSMA specifications define the platforms within this ecosystem, and the necessary conditions to be met by a platform to enter the ecosystem and thus interoperate.

How is it possible to check if a SM-DP/SM-DP+ is certified?

The SM-DP/SM-DP+ will be SAS certified according to the compliance process of the GSMA. The GSMA website[29] lists all accredited sites.

After a successful SAS certification, the SM-DP/SM-DP+ can apply to the CI to get a Certificate valid within the relevant ecosystem.

Will there be multiple CIs in the Consumer and/or M2M Architectures?

Consumer solution products:

> Currently the support of multiple CIs is ensured, but for the moment there is a single Root CI managed by GSMA and implemented by Digicert.

M2M solution products:

> The support of multiple CIs is expected to be available with version 4.0 of the specification that should be delivered in 2018.

Where can the list of GSMA compliant products and vendors be found?

The list of SAS accredited sites can be found on the GSMA website[30] and the list of GSMA Consumer solution compliant products can be found at the InfoCentre[31] which is for GSMA members only.

How can an operator be sure its Profile will work in a targeted eUICC?

Operators can define Profile configurations to optimise operation with different eUICCs embedded in devices. The GSMA Remote SIM Provisioning allows an ‘eligibility check’ of the eUICC and device capabilities to permit creation and download of an appropriate Profile. In addition, operators may use a specific Profile to provide specific services (examples include NFC, PKI) to their customer. Profiles should be created according to the SIMalliance Interoperable Profile package specifications[32].

[29] https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme/sas-accredited-sites-list

[30] https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme/sas-accredited-sites-list

[31] https://infocentre2.gsma.com/gp/og/STF/CRT/Pages/GSMA-RSP-Compliance-Products.aspx

[32] http://simalliance.org/euicc/euicc-technical-releases/

What is an activation voucher or activation code for Consumer solution?

An activation voucher or activation code is usually a QR code, supplied by the operator, which can be used by the end user to download a subscription Profile to a Consumer device.

How is this activation voucher used to download a subscription Profile?

After reading the QR code using its camera and a supporting application, the device is able to connect to the SM-DP+ named in the voucher and allows the eUICC to initiate a Profile download. The download will be made for the specific eUICC of the device. The activation voucher can be printed on a piece of paper, sent to the customer by email (after completing the activation process), or displayed on a screen (e.g. at the Point of Sale). All these options are viable, depending on the desired customer experience.

Who is the owner of the eUICC?

The eUICC, if embedded in the device, is part of the device and will thus be owned by the device-owner. However, like the main device operating system, the eUICC firmware is licensed to the subscriber by various parties.

Who is the owner of the Profile?

eSIM allows the operator to download and manage their Profiles containing the subscription credentials and potentially some applications. The operator is the owner of the Profile and licenses its use to the subscriber.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601