A guide to **eSIM Architectures**

Contents

1. Executive Summary

GSMA

Executive Summary

Since eSIM technology was first proposed by the GSMA, three different architectures for eSIM technology have been developed. In 2014, the GSMA published the first eSIM Machine-to-Machine specification, followed by the eSIM Consumer Specification in 2016 and has just recently published the architecture and technical specification for eSIM IoT in May 2023. The architectures for these specifications each offer specific benefits tailored to the sectors they are targeted at:

Benefits of M2M architecture

This architecture does not depend on the active participation of the Device user. As the profile can be remotely enabled or disabled directly by the Operator without user interaction. Additionally, the profile can be locally enabled by the Device in a specific use case. Therefore, this architecture can cover the eCall use case in the automotive sector, in which an emergency call is automatically triggered in the event of an accident. The Device service provider, such as the vehicle manufacturer or car rental company, can remotely manage the profile, enabling, disabling or deleting it, as necessary.

Benefits of Consumer Architecture

This architecture gives the Device user full control over the profile management, so that they can enable, disable, delete and swap a profile, as they require. Additionally, it enables multiple profiles at the same time e.g.: to attach to two different Operator networks data connection. That makes this architecture well-suited to provide global and multiple connectivity to a wide range of consumer Devices, from laptops and tablets to small wearable Devices, such as a smartwatch.

Using an eSIM reduces the space required for the SIM, meaning these consumer Devices can contain larger batteries. It also removes the need for a SIM tray, so it is easier to make the consumer Device waterproof. Both space reduction and SIM tray-less features are key requirements to provide connectivity to wider consumer Devices.

Using an eSIM reduces the space required for the SIM, meaning these consumer Devices can contain larger batteries. It also removes the need for a SIM tray, so it is easier to make the consumer Device waterproof

Benefits of the IoT Architecture

The eSIM IoT Architecture can be used to provide connectivity to a wide range of IoT Devices that lack a user interface and/or rely on a low throughput network, such as LPWAN or NB-IoT. In this architecture, the profiles are remotely controlled by a component called an eIM (eSIM IoT Remote Manager), which can enable, disable or delete profiles as required. Multi eIM associated with a single eUICC are permitted which reduces integration time and makes it easier to switch connectivity providers, handle bulk profiles and queue profiles operations. Moreover, this architecture provides the enterprises the same flexibility and control as consumers for IoT Devices, thus marking a significant advance for IoT implementations.

Multi eIM associated with a single eUICC are permitted which reduces integration time and makes it easier to switch connectivity providers, handle bulk profiles and queue profiles operations

1.1

Abbreviations

Terms	Description
eSIM	Embedded SIM
M2M	Machine to Machine
eIM	eSIM IoT Remote Manager
IoT	Internet of Things
eUICC	Embedded Universal Integrated Circuit Card
UICC	Universal Integrated Circuit Card
LPWAN	Low Power Wide Area Network
SM-DP	Subscription Manager – Data Preparation
SM-SR	Subscription Manager – Secure Routing
LPA	Local Profile Assistant
SM-DS	Subscription Manager – Discovery Server
IPA	IoT Profile Assistant
NB-IoT	Narrow Band IoT
eCall	Emergency Call
SM-DP+	Subscription Manager – Data Preparation+

2. Introduction

GSMA

Introduction

This guide to eSIM (embedded SIM) architectures is designed to educate senior decision makers and the eSIM ecosystem on the three alternative architectures, the rationale behind their creation, the benefits and value they bring to the industry and individual businesses. It also aims to address eSIM myths and showcase how eSIM technology is empowering the industry.

eSIM technology employs remote SIM provisioning functionality embedded in an universal integrated circuit card (UICC) chip, which may be either attached to a Device or deployed in a removable chip.

Although an eSIM is technologically different from a physical SIM, its primary purpose is the same: it authenticates the Device to make calls, send messages, and access the Operator's network seamlessly.

An eSIM offers the following benefits:

End User:

- Purchasing and activating eSIM over the air
- Convenient global connectivity
- Reduce electronic and plastic waste

Device:

- More exciting and accessible product design
- Hardware Space-saving solutions
- Simplified installation and deployment

Operator:

- Supply chain costs reductions
- Security and robustness solutions
- Universal remote activation

> Although an eSIM is technologically different from a physical SIM, its primary purpose is the same: it authenticates the Device to make calls, send messages, and access the internet seamlessly.

3. The Three eSim Architectures

The Three eSim Architectures

The three GSMA eSIM Architectures are carefully designed to perform remote eSIM provisioning and to optimise the interoperability, security, integrity and trust for specific sectors and users, while simplify the eSIM Solutions, making it easier for operators and their customers.

They are all designed to perform remote eSIM provisioning and to optimise the interoperability, security, integrity and trust of the solution for the end user.

3.1

M2M Architectures

Technical description

The M2M eSIM Specification is designed for Devices that may operate without a user and have no user interface. The main elements of the M2M architecture are the Operator, the eUICC (eSIM) in the Device, Subscription Manager - Data Preparation (SM-DP), and Subscription Manager - Secure Routing (SM-SR) modules. M2M Remote SIM provisioning was the first eSIM specification to allow an operator profile to be downloaded over the air.

The main components of the architecture:

- The operator triggers the profile download, and requests profiles are enabled, disabled and deleted.
- The SM-DP generates and encrypts the profile and performs eSIM profile download. Additionally, the server can enable, disable and delete the profile remotely.
- The SM-SR (secure routing) manages the eUICC and acts as a proxy to send the encrypted profile received from the SM-DP to the eUICC. Additionally, this server can enable, disable and delete the profile upon request from the Operator or M2M service provider. The eUICC decrypts and installs the profile sent from the SM-DP, and executes all enable, disable and delete commands sent by the SM-DP+ or SM-SR.

Use case:

The main use case is enabling eCall in the automotive sector: an emergency call profile needs to be automatically and locally enabled by the Device in the event of a vehicle accident.

? How does it work – push model

The operator sends the profile data and credentials to the SM-DP.

The SM-DP generates the profile based on the operator's data, the profile is encrypted with a symmetric key and sent to the SM-SR. The SM-SR sends the profile to the eUICC, which decrypts and installs the profile.

The communication is encrypted end-to-end from the SM-DP to the eUICC, and only the eUICC is able to decrypt the profile. The SM-DP belongs to the operator.

The SM-SR could be provided by the operator or, in some cases, the Device service provider, such as a rental car company or car manufacturer.

The operator or the M2M service provider manages the profiles, enabling, disabling or deleting them.

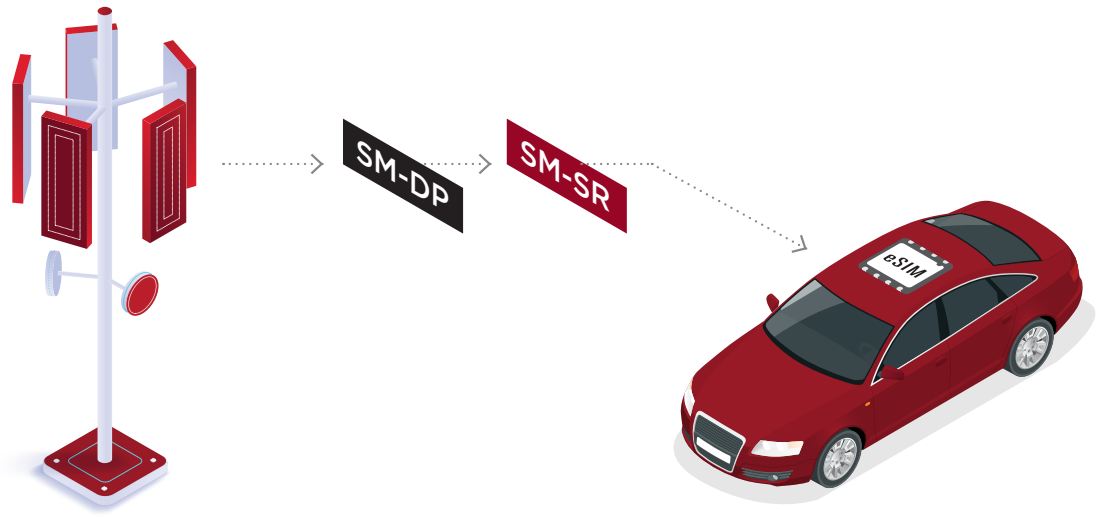
+ Benefits of M2M Architecture

This architecture is a device service provider centric architecture where the device user does not need to interact to perform a profile management operations. As the profile can be enabled or disabled directly without user intent, this architecture can cover the eCall use case. The device service provider can manage the profile, enabling, disabling or deleting the profile, as necessary. This architecture can be used to provide connectivity to devices for the automotive or utility industry.

– Benefits of Consumer Architecture

This architecture is a consumer/user-centric architecture that provides gives the device user full control over the profile management operations. The user can enable, disable or delete a profile, as they require. This architecture can be used to provide connectivity to a wide range of consumer devices from laptops to small devices, such as a smartwatch.

Figure 1
Push model



3.2

Consumer Architectures
Technical description

The Consumer eSIM specification is designed for use in consumer Devices, such as smartphones and tablets, where the user initiates the addition of a new profile or a change of profile. The main element of the consumer architecture is the Subscription Manager– Data Preparation+ (SM-DP+) component.

For profile management, there is a Local Profile Assistant (LPA), a mobile application residing either on the Device or the eUICC that serves as a proxy between the SM-DP+ and the eSIM and allows the user to enable, disable, delete, or download the profiles via SM-DS, QR code, or default SM-DP+ address installed in the eUICC. There is also an optional module called Subscription Manager – Discovery Server (SM-DS) that ensures a better user experience for profile downloading in certain use cases.

The main components of the architecture:

- The operator sends the profile data to the SM-DP+
- The SM-DP+ generates the profile from the operator data and encrypts the profile.
- The LPA software on the Device captures the user's actions, sends them to the eUICC and sends the encrypted profile to the eUICC
- The eUICC decrypts and installs the profile sent from the SM-DP+, and executes all the enable, disable and delete commands from the user.
- The user, via the LPA, triggers the install, enable, disable and delete operations of the profile.

Additional component:

As there isn't a SM-SR in the Consumer Architecture, a mechanism is required to link the Device with the SM-DP+ to download the profile. The SM-DS performs this role, providing the Device with the SM-DP+ address from which a profile is waiting to be downloaded on to this Device.

Use cases:

- The first use case defined was to provide connectivity to wearable Devices, such as a smartwatch. Using an eSIM reduces the space required for the SIM, meaning these Devices can contain larger batteries. It also removes the need for a SIM tray, so it is easier to make the Device waterproof. The user can employ the bigger screen of their smartphone to select a profile, which can then be downloaded into the smartwatch via their smartphone.
- The other use case was to have multiple active profiles, potentially connected simultaneously to two different networks, in the same eUICC. As it enables more than one profile at the same time, this approach makes more efficient use of the eUICC's resources.

? How does it work – pull model

The user buys a phone online and subscribes to a service from an operator. The SM-DP+ prepares the profile for this customer/eUICC. The operator provides a QR code that the user can scan on the Device to connect the Device with the SM-DP+. The SM-DP+ sends the encrypted profile to the LPA on the Device prior to a server authentication by the LPA.

The LPA sends the encrypted profile to the eUICC. The communication is encrypted end-to-end from SM-DP+ to the eUICC, and only the eUICC is able to decrypt the profile.

The eUICC decrypts and installs the profile. The user can now locally enable or disable the profile as required.

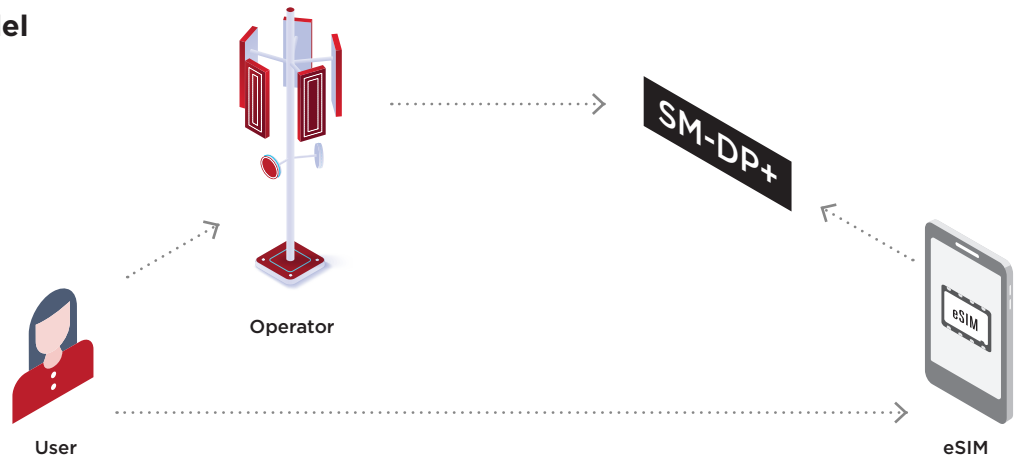
+ Benefits of Consumer Architecture

This consumer/user-centric architecture gives the user full control over the profile management. The user can enable, disable or delete a profile, as they require. This architecture can be used to provide connectivity to a wide range of consumer Devices from laptops to small Devices, such as a smartwatch.

– Disadvantages of Consumer Architecture

There are some constraints on IoT Devices, particularly those Devices without a screen through which a user can interact with the Device. Additionally, some IoT Devices are located in places where it would be difficult or impossible for a human to perform local operations. The Consumer Architecture is, therefore, not suitable for this type of IoT Device, which requires an entity to perform remote profile management.

Figure 2
Pull model



3.3

IoT Architecture
Technical description

The eSIM IoT specification is designed to be used in IoT Devices that are network-constrained or user interface constrained. This specification is based on the Consumer eSIM specification with a few notable differences. In the eSIM IoT specification, the LPA component of the Consumer specification is separated into two modules – the IPA (IoT Profile Assistant) and the eIM (eSIM IoT Remote Manager). The IPA will be on the IoT Device or the eUICC. It serves as a proxy between the eSIM and SM-DP+ for direct profile download as consumer but also it serves as a proxy between the eSIM and the eIM. To remotely enable, disable, delete profiles, and trigger profile downloads, the eIM sends profile state management operations to the eSIM. The eIM, which can facilitate the management of a single IoT Device or a fleet of IoT Devices, may be employed by an IoT OEM to manage its Devices.

The main components derived from the Consumer Architecture

- The operator sends the profile data to the SM-DP+.
- The SM-DP+ generates the profile from the operator data and encrypts the profile.
- The SM-DS links the IoT Device with the SM-DP+ from which the profile will be downloaded.
- The eUICC decrypts and installs the profile sent from the SM-DP+ or IoT Manager, and executes all the enable, disable and delete commands from the IPA

New components

- The eIM (eUICC IoT Manager) is a component that triggers profile downloads, and enables, disables and deletes the profiles. It is a modified components from the LPA in Consumer Architecture that emulates the user intent feature.
- The IPA is software on the IoT Device or eUICC, which is similar to the Consumer LPA, except the IPA does not need to capture the user intent as this feature has been moved to the eUICC IoT Manager.

A hight percentage of the eUICC functionality is based on the Consumer Architecture, with the rest coming from the new features and functionality required for the IoT ecosystem.

Use cases:

- To support IoT Devices that lack a screen through which to capture user intent.
- To support IoT Devices in locations where it is difficult to manually manage their profiles. Therefore, an external entity is required to manage the profiles remotely.

? How does it work – pull model

The user's eIM subscribes to a service from the operator. The SM-DP+ prepares the profile(s) for the eUICC. The operator provides a QR code that the eIM can scan via its own system to connect its Devices with the SM-DP+. After a server authentication, the SM-DP+ sends the encrypted profile to the IPA, either directly or via the eIM.

The IPA sends the encrypted profile to the eUICC. This communication is encrypted end-to-end, and only the eUICC can decrypt the profile.

The eUICC decrypts and installs the profile. The eIM can now remotely enable or disable the profile as required.

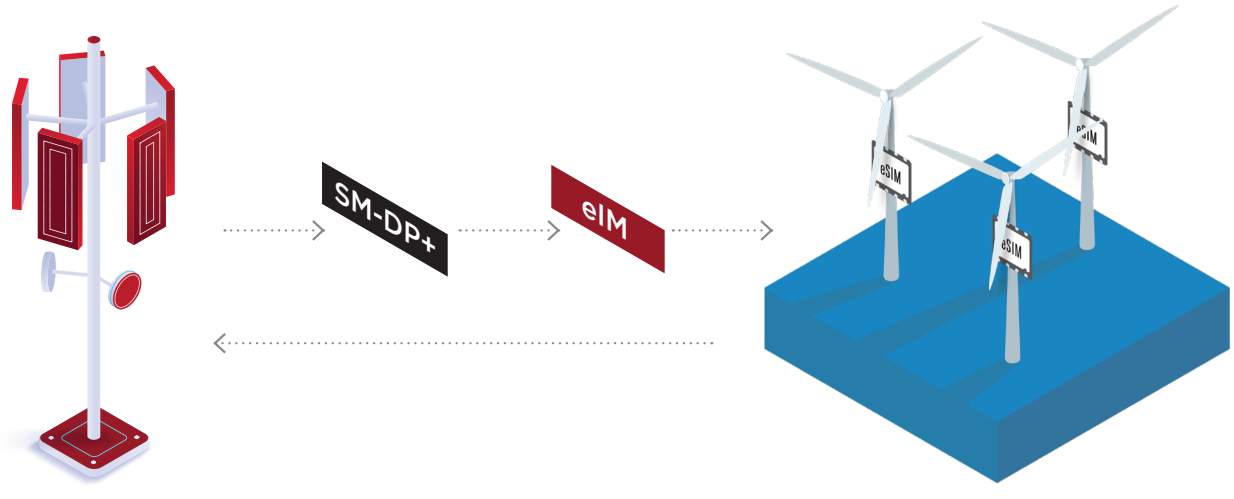
+ Benefits of IoT Architecture

This architecture is an eIM-centric architecture where there may be no device user directly link with the IoT Device and instead a remote manager component: the (eIM) has remote control of the profiles, and can enable, disable or delete profiles as required. This architecture can be used to provide connectivity to a wide range of IoT Devices that are network-constrained or user interface constrained.

+ Disadvantages of IoT Architecture

This architecture currently only covers IoT Devices that are network-constrained, or user

Figure 3
Pull model



interface constrained. The IoT Architecture may not be suitable for other type of IoT Devices with other specific needs. Nevertheless the architecture is expected to evolve to cover additional use cases and IoT Device types in the future.

Conclusions

Each of the three eSIM architectures discussed in this paper has been optimised for deployment in a specific sector of the connectivity market. In each case, the architecture has been carefully designed to simplify and streamline the deployment of eSIMs, making it easier for operators and their customers to realise the financial, environmental and design benefits of this technology.

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601