achelos

# eSIM Handbook

Use Cases & Technology

## Table of contents

# Introduction

## eSIM is the technology to digitise the plastic SIM card without jeopardising its role as the globally trusted security token for cellular network authentication.

As any other digitisation trend it creates opportunities for new market players to put forward innovative and challenging business models. The mission of **achelos** is to deliver the technology, expertise and development capacity required to enable these innovators.

We started the development for the IoT ecosystem targeting early adopters for niche use cases with a solution compliant with GSMA M2M specifications version 3.1. This solution was designed to be IoT service provider-centric with basic SM-DP functionality. The following major release early 2018 was the upgrade to version 3.2 with full GSMA functional scope ready for SAS-SM certification, as well as the introduction of HTTP-only communication with eSIM that does not require SMS-C integration. Based on the existing components we extended the solution for the consumer segment compliant with GSMA RSP (Remote SIM Provisioning) specifications version 2.2 that was first presented to the market with live demonstration on the Mobile World Congress Barcelona in March 2019.

As an Associated Member of the GSM Association (GSMA), **achelos** is actively contributing to the evolution of all relevant standards. We are committed to continuously upgrade the solution, incorporating new functionality and ensuring compliance with the evolving specifications. Our baseline strategy is to offer an independent, fully interoperable solution supporting eSIMs of any vendor and in any format – removable, embedded or integrated into the baseband processor (iSIM). This approach allows our customers to keep full control of the service and makes it easy and transparent for other parties to connect to it, whether operators, SIM and device manufacturers or platform providers. **achelos** works closely with eSIM vendors and device manufacturers to ensure this interoperability.

The functional scope of the Subscription Management solution is to securely handle the network access credentials in the form of MNO profiles and to provision these profiles to the eSIM in IoT and consumer devices. All core components are built in the form of microservices and loosely coupled, communicating via TCP/HTTP(S)/Message Broker interface for asynchronous and via TCP/HTTP(S) interface for synchronous data exchange, providing a high level of cohesion between the services. This approach has been selected to achieve excellent horizontal scalability of the complete system and to significantly improve system reliability.

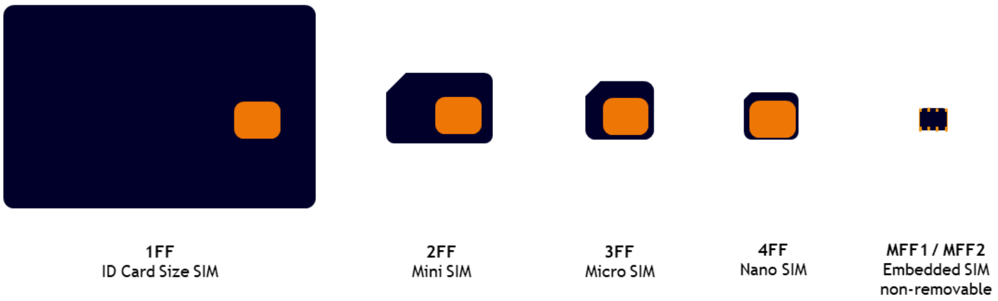
Beyond the software design we believe that a close integration of the components with the customer’s infrastructure and the support of the customer’s business processes and workflows are the keys for successful Subscription Management services.
**achelos** offers broad expertise beyond GSMA’s defined eSIM technology. We deeply understand the standards without being limited by them. Combining specialist knowledge of mobile network technology, carrier grade development, private and public cloud deployment as well as embedded OS and application development we build solutions that provide a competitive edge and exactly fulfil the needs of our customers. With complete in-house software development of all components we cover all services of the development project lifecycle from requirement analysis and design to development, integration and end-to-end testing.

As eSIM technology keeps maturing diverse parties across the mobile telecommunication and IoT landscape such as mobile network operators, connectivity and IoT service providers, chipset and device manufacturers need to define and implement a long-term strategy for eSIM management suiting their specific requirements. With this document we address this broad range of players; we cut down the extensive amount of available technical information to the relevant bits starting with the **generic features of eSIM** before addressing the specifics of **eSIM in IoT** and the **eSIM consumer** solution.

# Some Basics about eSIM

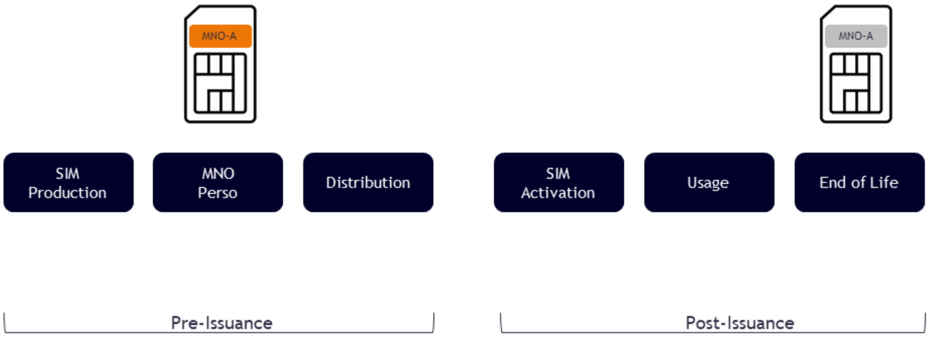
## When the first digital cellular mobile GSM network was launched in 1991 one of the key components of the system architecture was a removable smart card called SIM – the Subscriber Identity Module.

In the 2000's the increasing use of machine to machine (M2M) applications in tough industrial environments drove the need for non-accessible SIM cards, embedded and sealed within the device that could no longer be removed. So the European Telecommunications Standards Institute (ETSI) released a specification for M2M SIM in 2010 introducing the soldered form factor MFF (M2M Form Factor).



ETSI defined form factors

Difficult if not impossible replacement of the SIM (aka UICC), on the other hand, should not result in a permanent lock-in with the mobile network operator (MNO) issuing the cards since the lifetime of M2M devices can be very long with typically 10 years and more. This raised the requirement for a remote management solution of the complete “embedded SIM”, including network access applications and related credentials, for which the traditional (removable) SIM was unsuited.

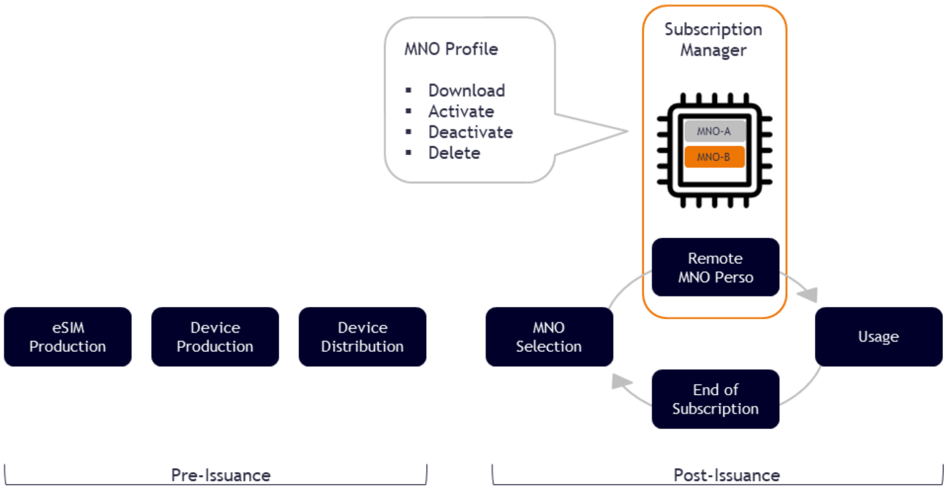


Traditional SIM lifecycle

The GSM Association (GSMA) took over the task of developing an industry standard for eSIM and the Subscription Management functionality. An important aspect of the GSMA specification design was to add remote profile management capabilities while maintaining the existing SIM ecosystem, including established ordering and activation processes, as well as compliancy with the well-known SIM standards developed by ETSI and 3GPP (3rd Generation Partnership Project). As a result the eSIM does not differ from the regular SIM card in terms of device and mobile network interfaces but is an extension of the existing technology.

**As defined by GSMA, the term eSIM refers to the explicit functionality of the operating system to store multiple MNO profiles and perform remote provisioning and management of these profiles after its issuance.**

This allows the separation of the profile (i.e. the connectivity) lifecycle from the hardware lifecycle, which is not available with the plastic SIM card that links the profile to the card at the time of production in a non-reprogrammable way.



eSIM lifecycle

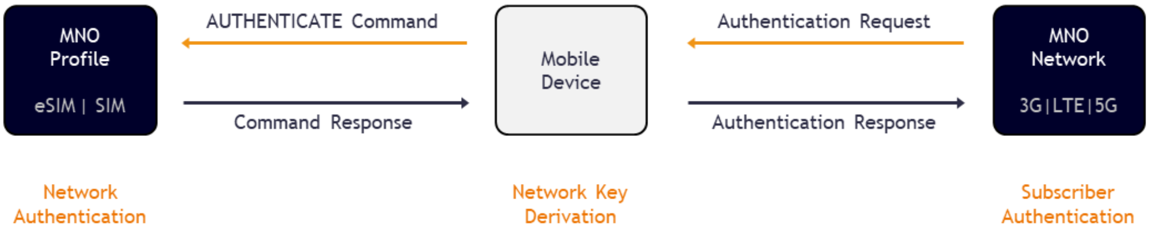
The new capability of remotely managing operator profiles needed to offer at least the same level of security as with existing SIM card management systems. GSMA selected time-proven Global Platform (GP) card management standards as well as state-of-the-art algorithms (Elliptic Curves Cryptography, AES) to make sure that eSIM technology would not compromise mobile network security standards.

**Although the term “embedded” may imply this, not every non-removable SIM is an eSIM. It is the functionality, not the form factor, that defines eSIM.**

The functionality can be made available as removable 2FF/3FF/4FF, embedded MFF1/MFF2 or in non-standardised formats. The evolution of cellular IoT technologies, especially LTE-M and NB-IoT for Low Power Wide Area Networks (LPWA), constantly seeks decreasing size and power consumption of devices and chipsets. This is driving the emergence of further eSIM form factors like the integrated SIM (iSIM/iUICC) where the eSIM functionality is implemented in a trusted environment of the System-on-Chip (SoC).

## Whether on SIM or eSIM, the MNO profile is, quite literally, the key to access a cellular network.

The core functionality of the operator profile, since inception of the first digital mobile standard GSM in 1990, is the storage of subscriber credentials and the implementation of algorithms used for network access authentication. Whether 3G, LTE or 5G - its role in the 3GPP Authentication and Key Agreement (AKA) remains a key feature of cellular mobile network security.



Authentication and Key Agreement (AKA)

The operator profile, in order to perform the authentication procedure, as well as numerous other tasks, must contain at least the following components:

MNO-SD (MNO Security Domain)

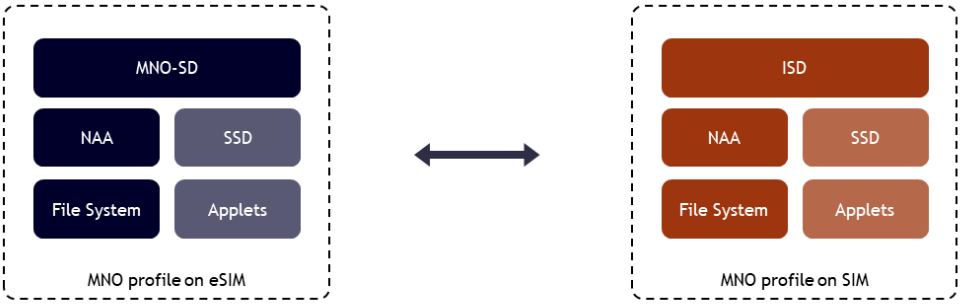
- managing the applications in the profile on behalf of the profile issuer, i.e. the mobile network operator (MNO)
- MNO-SD performs same function as ISD (Issuer Security Domain) on SIM

NAA - Network Access Application

- applications such as SIM, USIM and ISIM, which are selected by the device in order to access the related mobile network

File System - containing

- data files (Elementary Files - EF) that store subscriber and network information
- directory files (Dedicated Files - DF/ADF/MF) that allow functional grouping of files

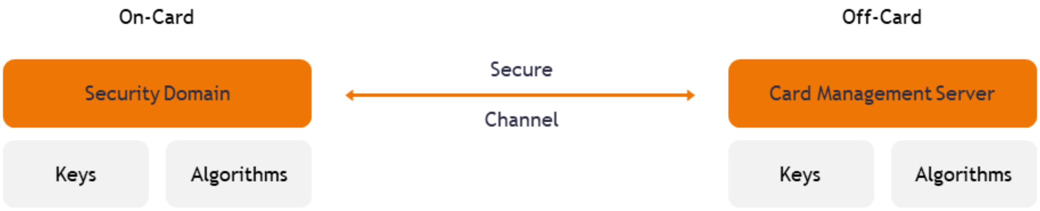


MNO profile on eSIM (eUICC) vs. SIM (UICC)

Further applications and Supplementary Security Domains (SSD) may also be part of the profile depending on the requirements of the operator controlling the profile.

**Decoupling the profile from the chip platform, which are bound together on SIM, requires a mechanism to securely separate the profiles and the eSIM platform.**

An established concept, the Security Domain (SD), provides just that and is central to the security architecture of eSIM - as well as smart cards in general.



Global Platform Security Domain

Security Domains are special applications containing key material and algorithms for cryptographic operations and have specific privileges managing the card’s applications and provide a trusted security level for the authentication of system entities as well as the protection of integrity and confidentiality of the communication.

The following distinct Security Domains for eSIM are defined:

ISD-R: Issuer Security Domain Root

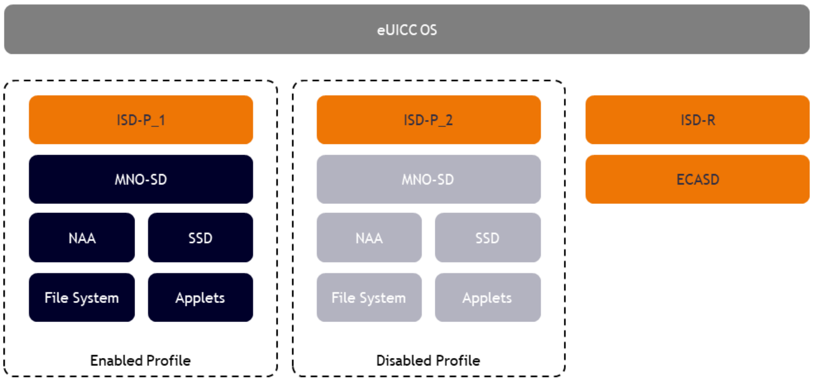
- performs eSIM management functions on ISD-Ps
- installed and personalized during eSIM production

ISD-P: Issuer Security Domain Profile

- hosts a unique profile
- only one ISD-P is enabled at any point in time

ECASD: eUICC Controlling Authority Security Domain

- the ECASD is installed and first personalized during eSIM production
- its services can only be used by ISD-R and ISD-Ps



eSIM (eUICC) architecture

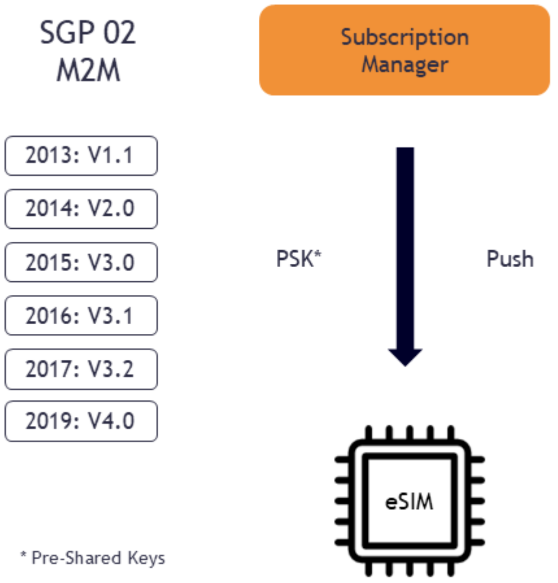
Designing eSIM based on established standards, for all its advantages, also creates challenges. SIM and eSIM, as defined today, contain complex functions for running and managing applications as well as legacy elements acquired over three decades of mobile technology evolution.

Especially in the highly cost sensitive IoT market there’s a clear need for solutions with a smaller footprint that focus on the core functionality of network authentication and more efficient profile download and management procedures without compromising overall network security.

# eSIM for IoT Devices

## In December 2013, the GSMA released version 1.1 of the "Remote Provisioning Architecture for eUICC" and the associated Technical Specification, creating the de-facto standard for Subscription Management systems for machine-to-machine (M2M) and IoT devices.

A strategic weakness of this specification was the absence of an interoperable profile download mechanism. This gap was closed with the release of the Interoperable Profile Description specification by SIMalliance in May 2015 and the GSMA SGP.02 v3.0 specification in June 2015.

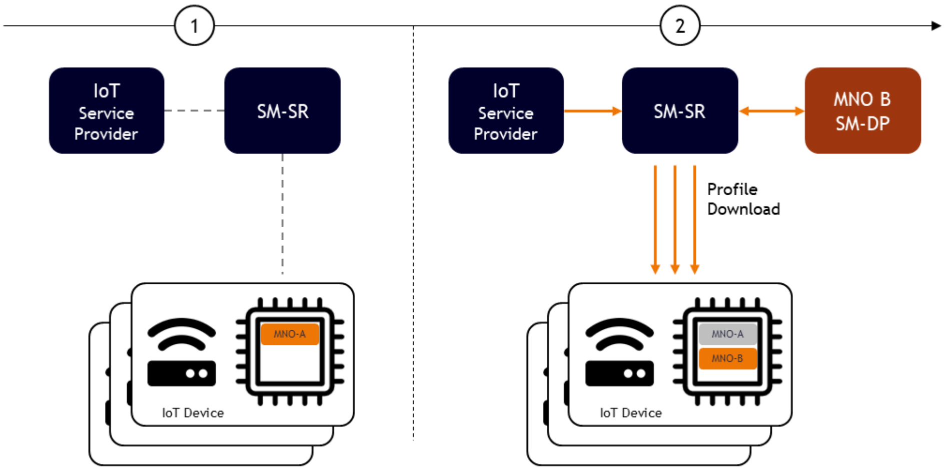


GSMA SGP.02 M2M

By loosening the dependencies between the eSIM and the managing platform, independence of the Subscription Management service from the eSIM manufacturing process became possible, creating opportunities for new players in the market.

## With IoT device lifetimes of 10 years or more the ability to switch the connectivity provider is essential.

The M2M subscription management functionality is illustrated below for one of the major IoT uses cases. Also known as “insurance”, this scenario prevents a connectivity lock-in for the IoT service provider. It allows switching connectivity from one operator to another either for an entire fleet of devices, or a subset thereof.



M2M subscription management

1. The device fleet of the service provider is provisioned with connectivity from MNO A and the eSIMs of the devices are registered with a Subscription Manager (SM-SR) of the IoT Service Provider’s choice.

2. At some point the IoT service provider decides to move the connectivity of the devices from MNO A to MNO B and puts the related contracts in place. In an automated process, the SM-SR requests profiles from the “profile data preparation” system of MNO B (SM-DP) and downloads the profiles to the selected devices. Whether the profile of MNO A remains on the eSIM or is deleted is part of the policy agreement between the parties.

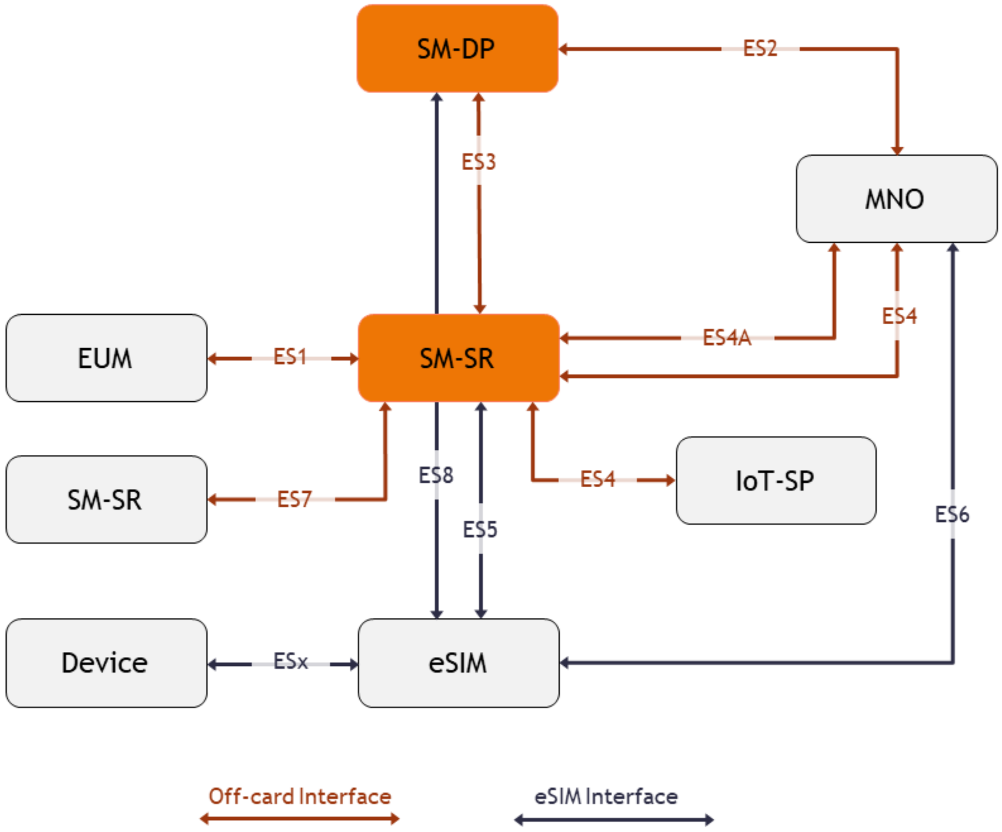
M2M subscription management requires cellular connectivity protocols; alternatives such as Wi-Fi are not supported - contrary to eSIM in consumer devices. Therefore the IoT eSIM must have an active profile at all times and an initial profile must be stored on eSIM already during production. This can be the final operational profile or a provisioning profile (aka bootstrap profile) with the dedicated function to download an operational profile once the device is activated.

**The GSMA M2M architecture is a server-driven push model that enables the centralised management of eSIMs and profiles by the owner of a fleet of devices.**

This management of profile and eSIM lifecycle requires the involvement of two system components.

The SM-DP (Subscription Manager Data Preparation) represents the profile owner and manages the mobile network operator’s profiles. It securely encrypts the network access credentials (i.e. the profile), ready for remote secure provisioning to a deployed eSIM.

The SM-SR (Subscription Manager Secure Routing) is in charge of eSIM management and represents the eSIM owner. It is also the entity that securely delivers the encrypted operator profile to the eSIM.

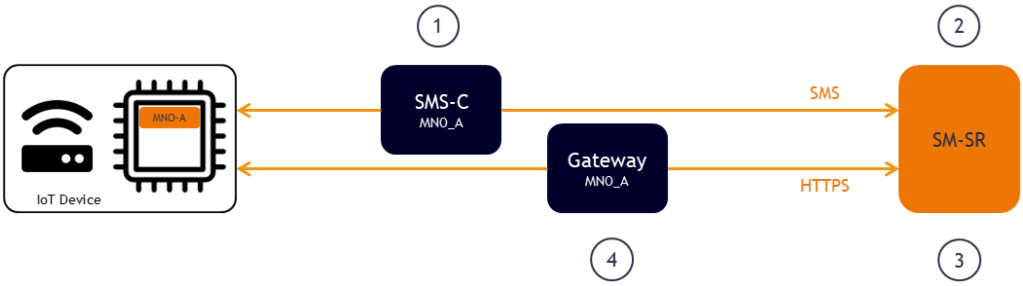


M2M Remote Provisioning System for IoT

The SM-SR manages the eSIM remotely during its lifetime using a specific set of operations, such as profile activation, deactivation or deletion.

**For remote communication with the eSIM the SM-SR uses SMS and packet data (HTTPS) transport channels of the mobile network.**

The SM-SR is free to select the most relevant transport protocol according to the capabilities of the targeted eSIM and device as well as the operation to execute.



Transport channels

The following network connectivity parameters are stored on eSIM to enable SMS and HTTPS transport for subscription management procedures:

1. SMS-C address
   identifying the SMS-C through which SMS are routed

2. SM-SR destination address (DA)
   the long or short code number to which eSIM originating SMS are sent

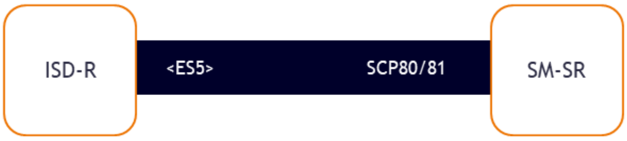
3. SM-SR IP address and port
   allowing the eSIM device to establish and maintain a network connection for HTTPS based communication

4. APN (Access Point Name)
   point of entry into an IP network

## The eSIM system was designed to offer a security level at least equivalent to the security of the traditional SIM and its application management systems.

GSMA incorporated GlobalPlatform standards to secure the eSIM interfaces ES5, ES6 and ES8 with the Secure Channel Protocol (SCP) mechanism.

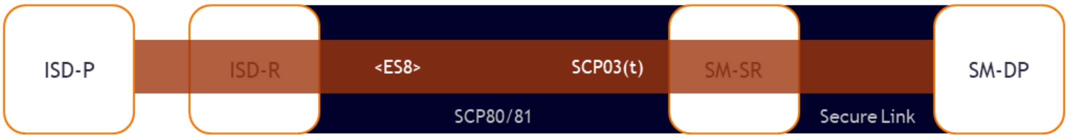
For ES5 functions (profile management) between SM-SR and ISD-R this depends on the selected transport channel. SCP80 is used for SMS (and the optional legacy protocol CATTP), while SCP81 is applied for TLS over HTTP (HTTPS).



ES5 interface security

Both protocols require algorithms and keys to be pre-shared in the system, meaning the keys are loaded into the ISD-R of the eSIM during production and then imported into the SM-SR.

For protection of ES8 functions (profile download) between SM-DP and ISD-P the Secure Channel Protocol SCP03 is used as well as the GSMA variant SCP03t. Since only the SM-SR can establish a remote transport channel with the eSIM, ES8 is always tunnelled.

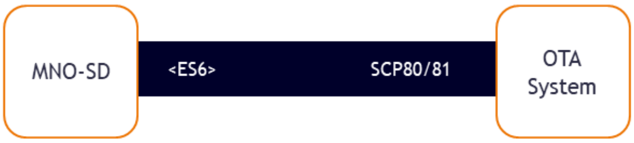


ES8 interface security

Contrary to the ISD-R, which is personalised during eSIM production with pre-shared keys, an ISD-P is typically created post-issuance and no initial keys are available to secure the communication.

Therefore, ES8 contains a procedure by which the SCP03(t) key set is established between the ISD-P and its related SM-DP. This is based on an elliptic curve key agreement scheme, also defined by GlobalPlatform, the so called “Key Establishment with Scenario#3-Mutual Authentication”.

The ES6 interface (update of profile components such as the profile connectivity parameters) uses the same secure channels as ES5, with SCP80 for SMS (and CATTP), and SCP81 for HTTPS. Besides the MNO-SD shown in the diagram, any other Supplementary Security Domain (SSD) of the profile can be used.



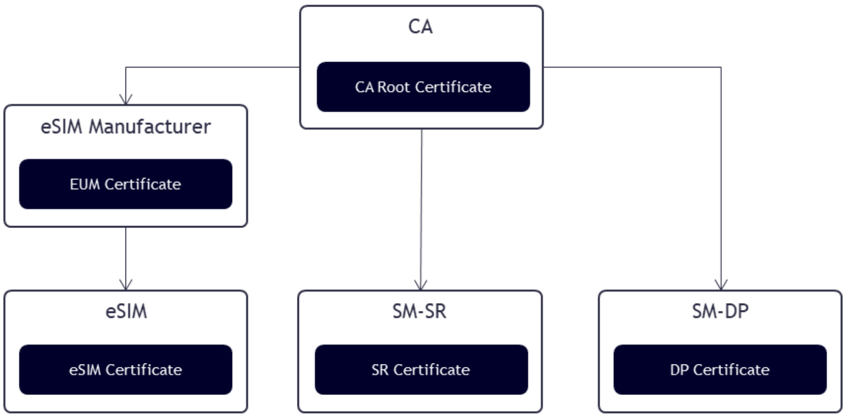
ES6 interface security

The OTA system is not covered by the GSMA specification. It may be a legacy system used for SIM as well as eSIM profiles. As with ES5, the keys for SCP80/81 must be pre-shared and are either loaded during the profile download procedure by SM-DP or by the EUM during eSIM manufacturing in the initial profile.

While the security of “on-card” eSIM interfaces is specified in detail, the “off-card” interface security affords more flexibility how to implement the required security level. As part of its Security Accreditation Scheme for Subscription Manager roles (SAS-SM) the GSMA has released several documents providing guidelines and requirements for security certification that provide detailed information about this area.

## To create trust between the different parties throughout the eSIM ecosystem GSMA has defined a Public Key Infrastructure (PKI) supporting the use of Certificates for authentication.

A Certificate Authority (CA) is acting as a trusted third party for the purpose of mutual authentication of all system entities, using a self-signed Root Certificate to verify certificates issued and signed by the CA.



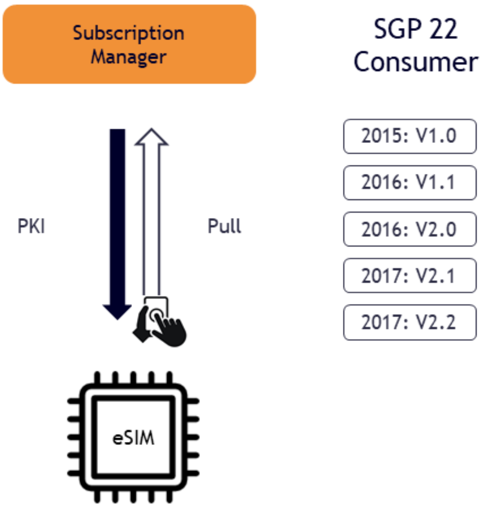
Certificate chains for IoT eSIM

The CA signs the certificate of the eSIM manufacturer (EUM) that becomes a sub-CA issuing the eSIM certificates. The CA also signs the operational SM-DP and SM-SR server certificates. This trust model is deployed in the global, open eSIM ecosystem using a GSMA recognised CA but also effectively secures closed systems with a private CA.

# eSIM for Consumer Devices

## The need to develop a set of specifications for consumer devices became urgent with the arrival of size-critical companion devices, most prominently smart watches.

In 2015, GSMA began work on the Subscription Management specifications for consumer devices, resulting in the release of the first version in December 2015, updated to v2.2 in 2017.



GSMA SGP.22 RSP (consumer eSIM)

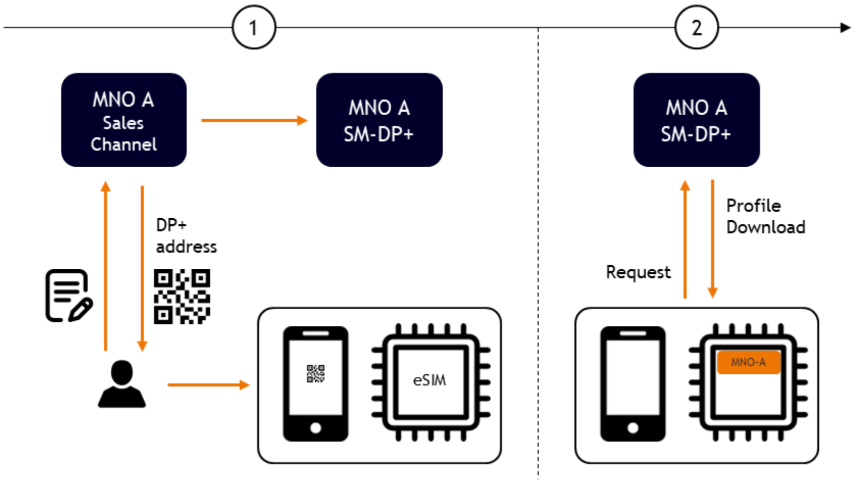
The existing IoT architecture had to be adopted to cater for the specific usage scenarios of the consumer market. While the connectivity change for IoT devices is driven by automated business rules in the backend and happens transparently for the user of the application (if there is even a human user) the management of the consumer device occurs only with the consent of its user. The user makes the connectivity choice, just as with the exchange of physical SIM cards on traditional devices.

Before any service can be provided a contract must be established between the user and a service provider, which also involves a subscriber enrolment procedure.
One of the central challenges for consumer devices remains to create a user-friendly experience without jeopardizing the security of the mobile ecosystem, ensuring compliancy with all legislative and regulatory requirements.

## Availability of devices with eSIM is not enough; operators have to build the use cases, infrastructure and processes for users to activate them.

The profile download process utilising a QR code consists of the following steps:

1. The user sets up a contract with a chosen mobile network operator, which provides instructions on how to connect the device to the operator's Remote SIM Provisioning system, the SM-DP+. These instructions also contain a QR code with the address of the SM-DP+.

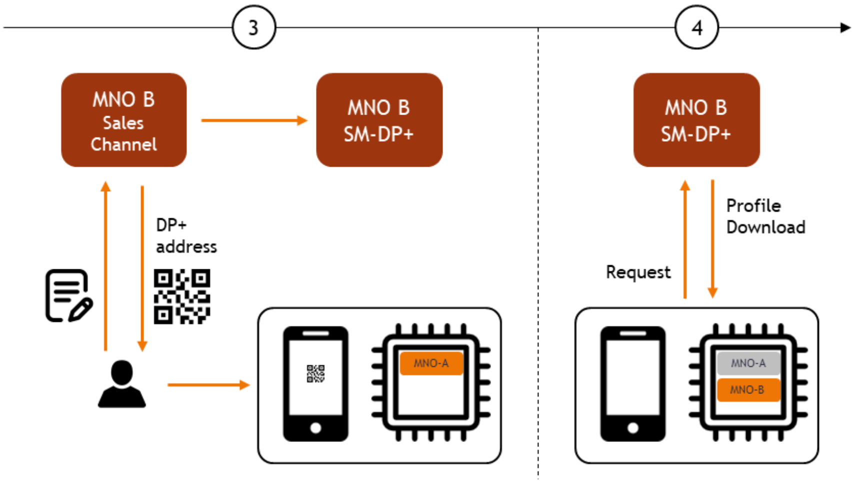


First profile installation via QR code

2. This allows the device (through a specific application called LPA - Local Profile Assistant) to connect to that system and the profile is securely downloaded to the eSIM. Once the profile is activated, the device is able to connect to the operator’s network.

Contrary to the M2M profile download, the eSIM does not require a pre-installed profile to enable mobile data connectivity; the device can utilise its Wi-Fi connection, or the connection of a paired device.

3. When the user wants to change the service provider, he or she sets up a contract with a new operator and in return receives a QR code. The user scans the code, allowing the device to locate the new operator’s SM-DP+.

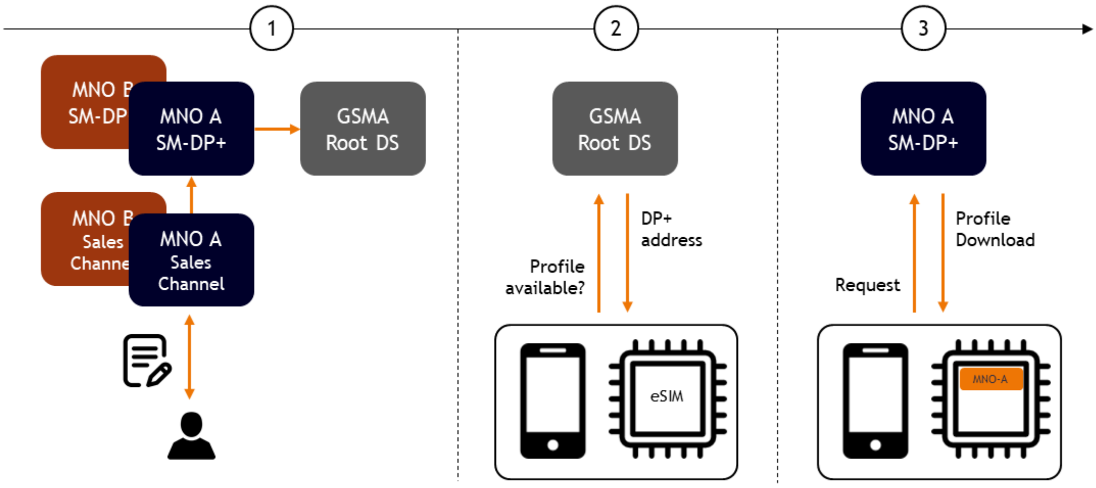


Second profile installation via QR code

4. The new profile is downloaded securely and the user is now able to switch between the two profiles installed on the device, connecting it to whichever MNO network the user prefers. This selection is also done through the LPA (Local Profile Assistant) of the mobile device.

To simplify the customer experience of connecting open-market consumer devices, the GSMA Root Discovery Service enables users with an established mobile subscription to download the profile without the need for a QR code.

1. Once the user has signed a mobile subscription contract with an operator, a profile is allocated in the operator's SM-DP+. The SM-DP+ informs the GSMA Root Discovery Service that it has a profile waiting for the user's device.



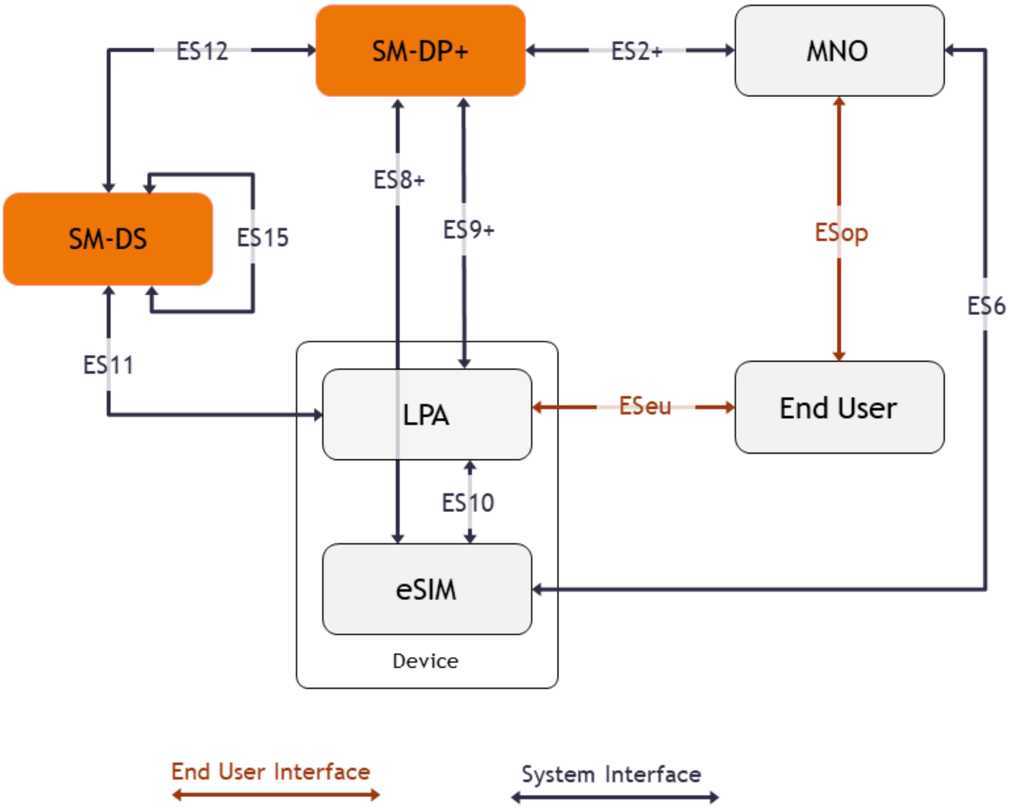
Profile installation via GSMA root DS

2. Through the device's LPA the user requests a check for a new profile. The device contacts the GSMA Root Discovery Service, receiving the response that a profile is waiting for the device on the SM-DP+ of the user's selected service provider.

3. The device contacts this SM-DP+ and the profile is downloaded and installed on its eSIM. Following profile activation, the user has access to the subscribed services.

## The system architecture for consumer eSIM puts the user, not the operator, at its centre for control.

The GSMA consumer architecture follows a client-driven pull model that enables control over remote provisioning and local management of operator profiles by the end user of the device.



Remote Provisioning System for consumer eSIM

As in the IoT solution, the consumer solution requires a central system role, the SM-DP+ (Subscription Manager Data Preparation plus) for the creation and protection of operator credentials, i.e. the MNO profile. However, as it encompasses the SM-SR functions for the physical transport link to the device it carries the “+” in its name, rendering the SM-SR obsolete in the consumer architecture.

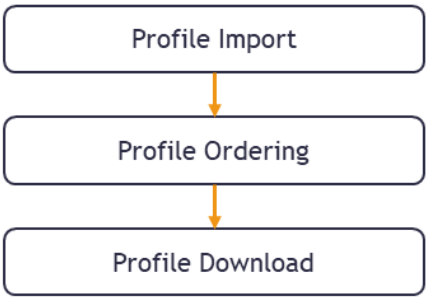
The optional SM-DS (Subscription Manager Discovery Server) is specific to the consumer solution. It enables automated profile discovery, depending on the activation procedure selected by the mobile network operator.

Another role specific to the consumer solution is the Local Profile Assistant (LPA). This element must be implemented as an application on the device but can optionally also be available on the eSIM itself. Dedicated LPA components facilitate the interaction of the eSIM with these system roles:

- End user through LUI (Local User Interface)
- SM-DP+ through LPD (Local Profile Download)
- SM-DS through LDS (Local Discovery Service)

**The core procedure in the consumer eSIM system is the remote provisioning of the operator profile. It is designed to ensure a high and consistent security level across the entire ecosystem.**

The generic profile process flow in the SM-DP+ consists of the following steps:

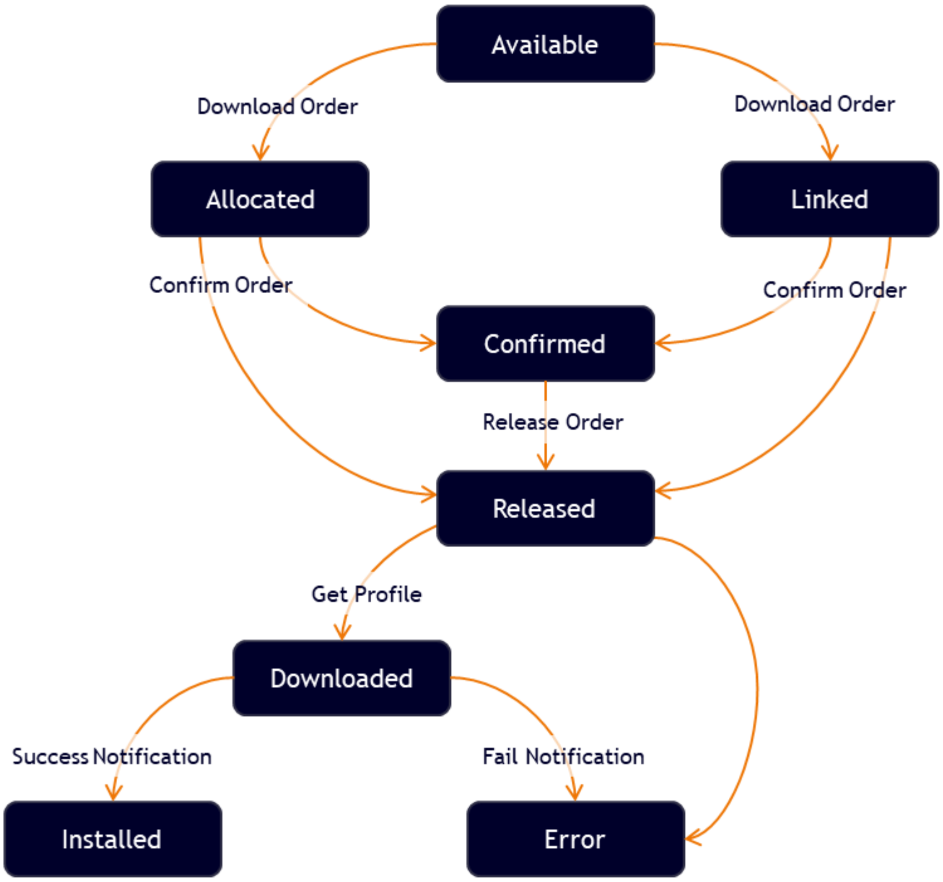


Generic process flow

Profiles are imported into the SM-DP+ (or generated in SM-DP+ based on imported profile subscription data). At this stage they become available within the system.

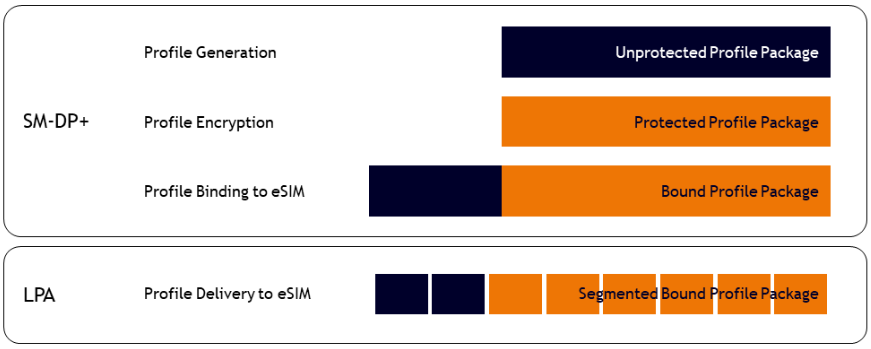
Before a profile can be downloaded to a device it must be ordered by the operator in several steps, from the initial download order to confirmation and release. Once a profile has reached the state “Released” it is ready for download when requested by the user.

The diagram below illustrates a profile’s lifecycle in SM-DP+ with the available system operations and resulting profile states:



Profile lifecycle

From generation to installation into eSIM the profile package takes different formats, ensuring the protection of the profile's content.



Profile package formats

1. The SM-DP+ generates the Unprotected Profile Package (UPP) based on the operator defined profile structure and subscription data. The result is a block of data in SIMalliance defined format.

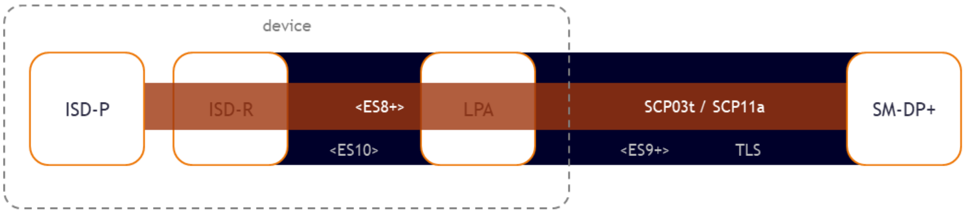
2. By encrypting the UPP in Global Platform secure channel SCP03t format the SM-DP+ generates the Protected Profile Package (PPP) using Profile Protection Keys (PPK) for confidentiality and integrity protection.

3. Once the target eSIM is known the SM-DP+ can generate the Bound Profile Package (BPP) by prepending the PPP with eSIM specific information.

4. When the BPP has been delivered to the LPA of the device it generates the Segmented Bound Profile Package (SBPP), a sequence of APDUs for loading the profile into the eSIM.

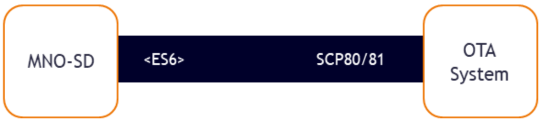
The consumer system interfaces and their security have been built on the principles of the existing interfaces of the IoT solution. However, many functions specific to the consumer solution required existing interfaces to be extended as well as the definition of a number of new ones.

The functions of the ES8+ interface, responsible for profile delivery to eSIM, are addressed through a secure channel established between the SM-DP+ and the eSIM and is tunnelled over the interfaces ES9+ and ES10 as shown below:



ES8+/ES9+ interface security

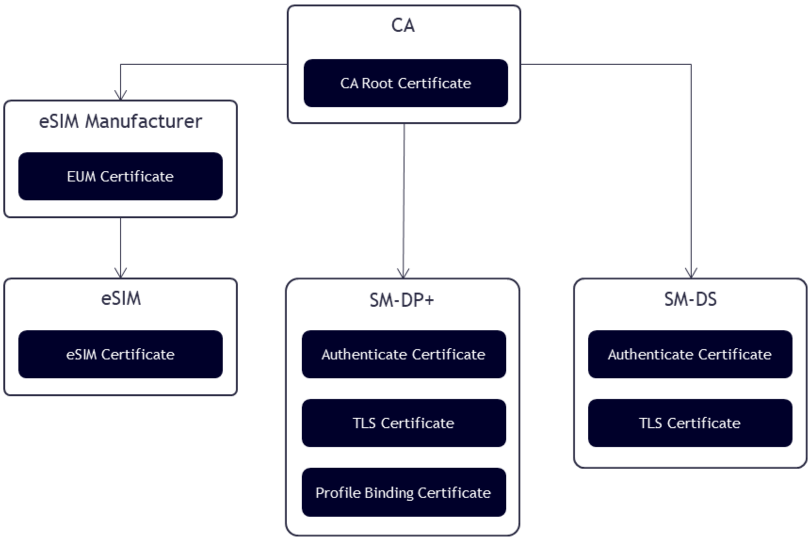
The interface ES6 between the operator and their enabled profile in the eSIM allows the MNO to modify the profile using legacy OTA mechanisms through secure channel protocol SCP80/81 in the same way as in the IoT solution.



ES6 interface security

The system interfaces (ES2+, ES9+, ES11, ES12 and ES15) are secured by Transport Layer Security (TLS) based on system certificates and their related pairs of public and private keys.

As with the IoT solution all certificates defined within the ecosystem have a validation chain whose root is a certificate from the Certificate Authority (CA) that is acting as a trusted root for the purpose of authentication of all system entities.



Certificate chains for consumer eSIM

The CA is an entity selected by and acting on behalf of the GSMA. Only parties that undergo the required GSMA security certification (SAS-SM for Subscription Management Service and/or SAS-UP for eSIM production) can receive the respective certificates from the CA and thereby become part of the consumer ecosystem.

# Abbreviations

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| AES | Advanced Encryption Standard |
| ECASD | eUICC Controlling Authority Security Domain |
| ECC | Elliptic Curves Cryptography |
| EIS | eUICC Information Set |
| ETSI | European Telecommunications Standards Institute |
| eUICC | Embedded Universal Integrated Circuit Card (UICC) |
| EUM | eUICC Manufacturer |
| GSMA | GSM Association |
| LPA | Local Profile Assistant |
| NAA | Network Access Application |
| PSK | Pre-shared key |
| SAS | Security Accreditation Scheme (GSMA) |
| SCP | Secure Channel Protocol |
| SM-DP | Subscription Manager Data Preparation |
| SM-DS | Subscription Manager Discovery Service |
| SM-SR | Subscription Manager Secure Router |

achelos

For more information, visit:

connect.achelos.com