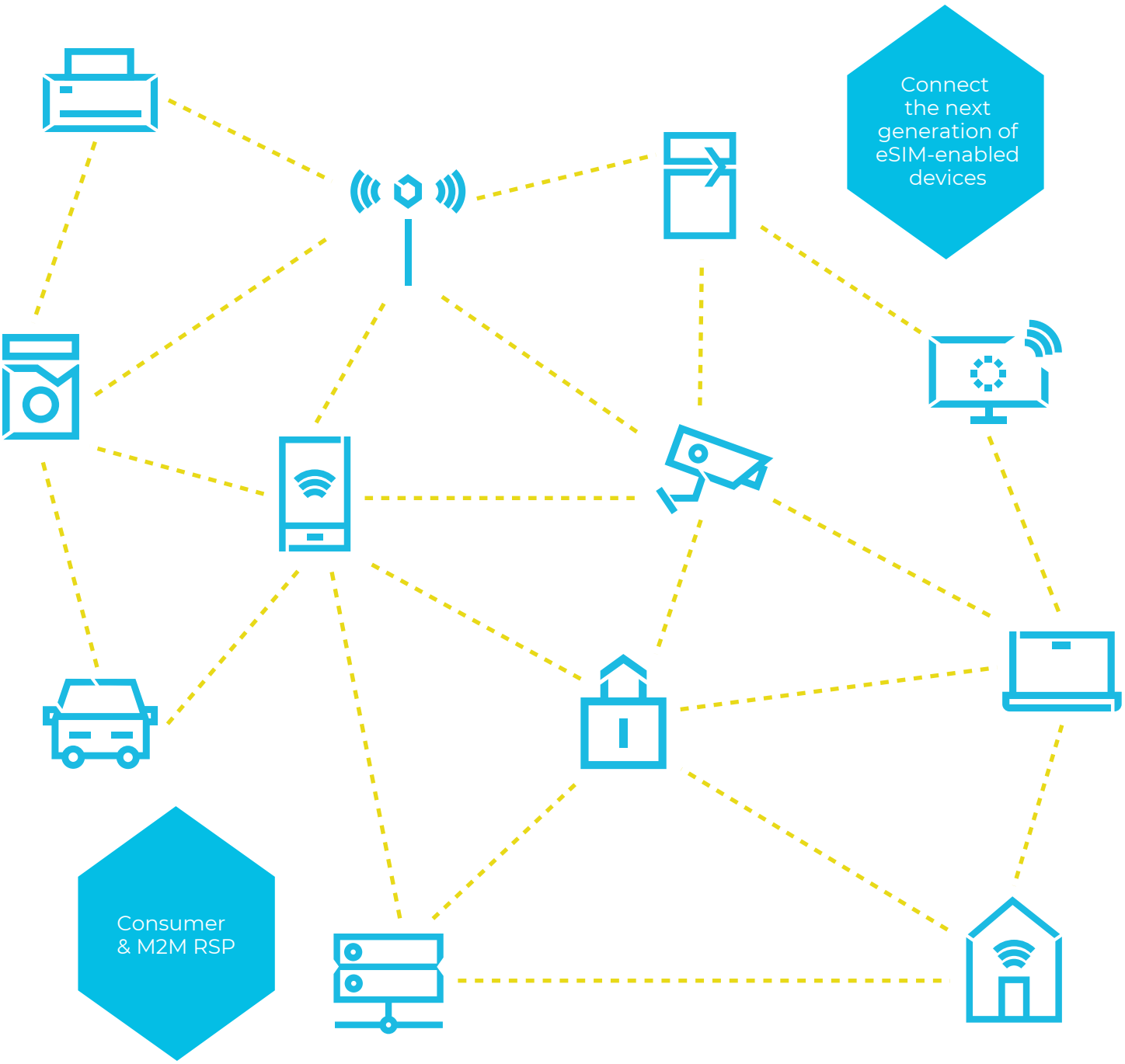
How Remote SIM Provisioning Works

Kigen

November, 2020

eBook



Contents:

- 3 Introduction
- 4 From SIM cards to eSIM and iSIM
- 6 Building the RSP vision
- 7 Key RSP terms defined
- 9 Inside the M2M RSP solution
- 14 Consumer pull: users request RSP
- 17 M2M RSP use cases
- 18 RSP streamlines deloyment
- 19 Integrating M2M RSP

This eBook summarizes the concepts, key specifications and processes of RSP. Also discussed are innovative ideas for capturing more IoT business opportunities.

Introduction

Trust is a crucial element for cellular networks, so every device attempting to join them must be positively identified and securely authenticated. Remote SIM provisioning, or RSP, is a proven approach for managing secure device identity through embedded SIMs (eSIMs) and integrated SIMs (iSIMs).

The Internet of Things (IoT) is predicted to reach critical mass by 2035, with a substantial portion of this growth coming from cellular connected devices. This is both an opportunity and a challenge for those operating in the IoT space, as traditional SIMs come with certain limitations. One of the key challenges is the need for a physical change of SIM cards to change networks.

RSP offers a secure, robust and highly scalable solution to address the traditional SIM challenges as it allows device owners to remotely change network operators by securely switching profiles over-the-air. This remote profile management removes the need for physical access enabling IoT devices to benefit from new SIM form factors that are deeply embedded, smaller and more reliable such as the eSIM and iSIM.

RSP was first brought to market for machine-to-machine (M2M) devices implementing eSIM technology. Consumer RSP specifications followed, prompting mainstream adoption of eSIM technology.

These specifications help build trust across rapidly expanding mobile, M2M and IoT ecosystems in several ways:

Mobile network operators (MNOs) can allow safe onboarding of devices to their networks without knowing the devices, yet still be confident that network security and its integrity won't be compromised.

Device and module makers can sell the same product anywhere in the world without having to procure multiple variants of SIMs for different networks, enabling a 'build once, ship anywhere' commercial strategy. Post-issuance, they can make updates to devices (with the owner's agreement) and even provide new services remotely. The new SIM form factors can also help reduce the power consumption and cost of devices.

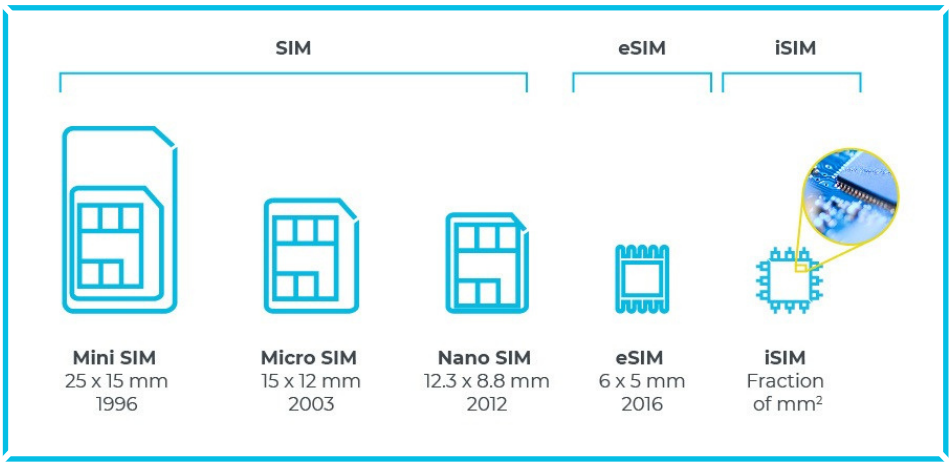
IoT service providers can tap into widely available cellular networks and benefit from new emerging cellular IoT technologies such as LTE-M, NB-IoT and 5G. This avoids the need to build infrastructure and instead allows focus on customer service and innovation.

Device owners can easily manage the connectivity of their devices and upgrade service plans remotely. This is a significant benefit where devices are not managed by the end user or are not readily accessible (for example, due to operational scale), making local device management cost prohibitive.

From SIM cards to eSIM and iSIM

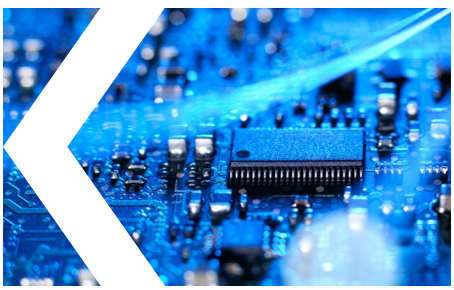
Before diving into concepts, let's briefly introduce eSIM and iSIM technologies, which support RSP capability.

SIM cards date back to the days of GSM phones, and were originally the size of a credit card. Phones and electronic devices shrank, and so did SIM cards, with successively smaller form factors. SIMs went from mini- to micro- to the nano-SIM form factor, with the latter being introduced in 2012. These changes reduced the plastic frame to just a border around the electronics and the metal electrical contacts were rationalized while maintaining form factor interoperability.



Evolution of the SIM

In GSM phones, SIM referred to dedicated hardware and software on a SIM card. With the introduction of UMTS 3G phones, a SIM became a software application running on universal integrated circuit card (UICC) hardware. A UICC is a type of smart card containing an embedded processor core, memory and cryptographic functions. UICCs can run multiple applications to perform a variety of functions.



Traditional SIM cards are themselves individually inexpensive, but require supporting components, processes and packaging. Accommodating devices must feature SIM slots or trays. SIMs are manufactured in audited secure facilities and personalized with the data provided by network operators. Network operators must stock and manage the distribution of SIM cards as well as train their customer services, retail and support personnel in SIM installation and troubleshooting. Physical handling occurs during deployment, with the risk of damage, tampering or loss.

Yet, the biggest drawback of traditional SIMs is that they typically host one network profile and physical swaps of SIMs are required to change from one operator to another. For someone deploying devices into many regions, local SIMs must be sourced from regional network operators and then distributed to and inserted into each device for every target destination of use.

This drawback is also shared by non-removable SIMs which don't support RSP and also only host one fixed profile each. OEMs or module makers, who wish to embed these SIMs during manufacturing, must source and stock different local SIMs from regional network operators for all the countries the device will operate in. Additionally, a device with this type of SIM is fixed to the same network for its lifetime, as a SIM swap is near impossible. The eSIM and iSIM are also non-removable physical form factors. The key difference is that they support RSP, which addresses the above-mentioned logistical and management challenges associated with traditional and single-profile SIM cards. They eliminate the plastic card, tray or slot frame and connector, which releases space on the device and allows for device size reduction. They also eliminate the potential for theft or damage.

When it comes to protecting the subscription credentials, both eSIM and iSIM are similar to traditional SIM cards.

Building the RSP vision

The core function of RSP is remote management (delivery, installation, enabling, disabling, deleting) of profiles with operator and subscriber data on devices. Prior to RSP, profile changes meant physically swapping SIM cards. Several motivations drove GSMA to create the RSP specifications:

Enabling non-removable form factors
RSP allows for a change of operator profiles on those form factors that are not designed to be physically accessed (eSIM or iSIM). Note that RSP can also be used on a capable removable UICC, since it is virtually equivalent to a non-removable one. Continuity of service is supported, as soldered down or integrated UICCs are more robust and offer greater theft protection when compared with traditional SIMs.

Quickly changing network operators
If the device owner wishes to use a different network, changing the eSIM profile is easy. Device owners can choose a new network rather than being forced to use the operator profiles set at the factory. They can also now switch network without having to physically access and replace their SIM cards.

Onboarding more IoT devices
According to market research firm IoT Analytics, the number of IoT devices on the market will reach 22 billion by 2025. Large numbers of these devices will be cellular enabled. eSIM and iSIM remove the barrier to rapid cellular device deployment, especially in applications spanning multiple networks.

Reducing lifecycle support costs
For a single application, IoT devices may be deployed by the thousand in far flung locations. Provided the right capabilities are in place, devices can be diagnosed and even updated remotely, avoiding costly service call

One more important consideration is whether a device is headed for a consumer or M2M environment. These use cases require two different RSP solutions. In this eBook, we'll focus on the M2M solution and briefly touch on the contrast with the consumer solution.

Key RSP terms defined

We'll recap on several terms already mentioned and also introduce definitions for key terms in the RSP solutions discussion that follows.

RSP - Remote SIM Provisioning

RSP is the secure management of network operator profiles on a device with an eUICC using over-the-air commands. Subject to the availability of network coverage/capacity and device capabilities, its functions include setting up secure communication channels to an eUICC and downloading, installing, enabling and deleting profiles. Profile data is protected end-to-end, at every point of the process. RSP requires digital certificates on both the device and server side, obtained only through completing GSMA certification steps. GSMA specifies two RSP solutions, one for consumer applications and one for M2M applications.

SIM - Subscriber Identity Module

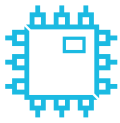
The SIM is the component that establishes secure device identity and holds network operator and subscriber data. Colloquially, SIM is often used to refer to the physical SIM card form factor containing a UICC with a single profile.

eSIM - Embedded SIM

A physical non-removable SIM that is soldered into a device. eSIM technology provides equivalent security to a conventional SIM card, with additional secure over-the-air update capability.

eUICC - Embedded Universal Integrated Circuit Card

An eUICC is a hardware component that contains a security architecture for SIM operation and profile storage. Most form factor implementations for eUICCs are packaged in solderable chips (eSIMs). eUICCs have two key additions compared to UICCs: they are updatable over-the-air and can store and manage multiple eSIM profiles.



iSIM - Integrated SIM

An iSIM is a physical non-removable SIM that is integrated into a secure enclave alongside the processor and modem on a system on chip (SoC). Delivering these three building blocks in one component further reduces the device footprint, power consumption and manufacturing costs.

EUM - eUICC Manufacturer

EUMs take data from the network operator, generate personalization data and personalize the eUICC. The following activities are involved (these can be carried out by a single organization or split between multiple vendors): card personalization preparation, input data handling, personalization data generation, card personalization and output file issuance. EUMs must have the appropriate GSMA security accreditation and hold the associated 6 certificate before they can deliver personalized eUICCs for use. Additionally, the EUM issuing the eUICC's RSP PKI certificate must ensure the eUICC product has achieved GSMA compliance from both a security and functional perspective.

Network operator profile

A profile enables access to a cellular network. It contains data that identifies the device to the network, plus network access applications with the required encryption keys for security. RSP-enabled M2M devices with eSIM technology are shipped with a bootstrap profile that allows them to establish an initial network connection to download another operational profile that the device will use.

SAS - Security Accreditation Scheme

GSMA works to promote security and interoperability of devices, lowering risks for network operators and device owners. They have created a Security Accreditation Scheme where ecosystem participants are certified against GSMA specifications. There are two auditing tracks: one certifying UICC and eUICC manufacturing processes and sites, and one certifying the hosting and operation of sites delivering subscription management services. This reduces the need for an MNO or IoT service provider to conduct its own audits of suppliers.

SAS-SM - Security Accreditation Scheme - Subscription Management

An SAS-SM audit looks at both the the implementation of the subscription management software and the integrity of the organization and facilities from where the remote SIM provisioning activities are conducted. This includes areas such as business continuity planning, personnel and physical security, processes for certificate and key management, and computer and network security procedures. Only when a supplier is certified can they obtain the required digital certificates that allow them to provide RSP services.

Digital certificates

Digital certificates can be issued for eSIM personalization upon successfully achieving the GSMA eSIM product compliance. These are used as tokens of trust for the eSIM's authentication with the RSP management servers.

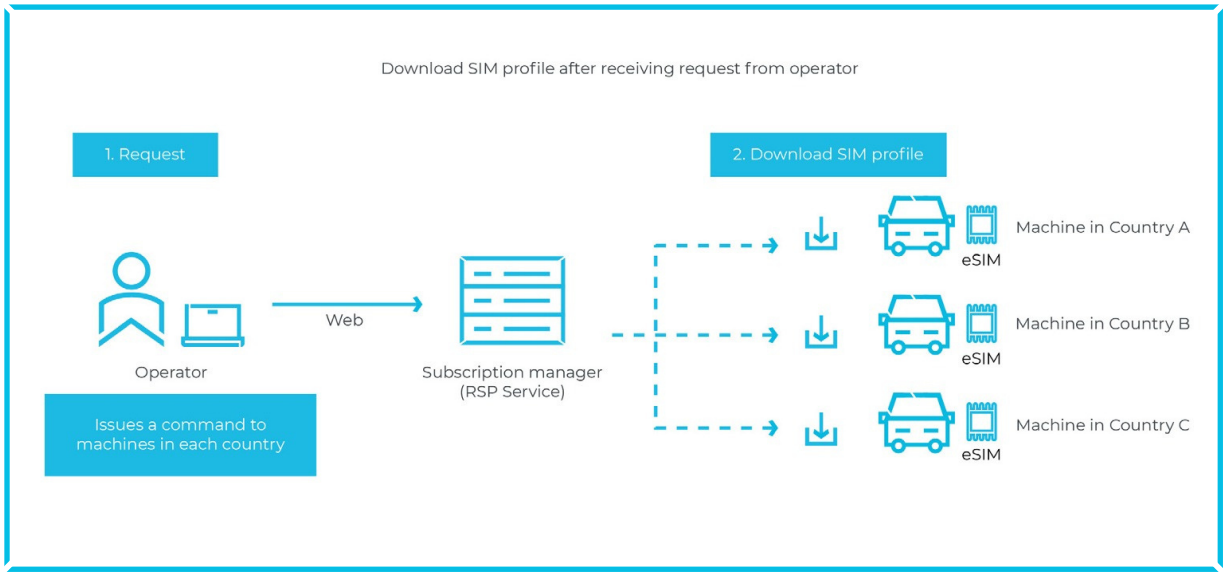
Off-card entities

A remote party and their servers that have the authority to establish a secure channel with an eUICC or security domain existing within, over which management can be achieved. Management of the eUICC or a security domain may be conducted directly or be dynamically delegated to another trusted off-card entity. Authority is granted through the issuance of PKI certificates and or the sharing of mutually issued cryptographic keys.

Inside the M2M RSP solution

With the conventional SIM card so entrenched in consumer devices and a pressing need for a solution supporting IoT device provisioning in automotive applications, GSMA chose to develop the M2M solution for RSP beginning in 2013.

Typically, once deployed, an M2M or industrial IoT device has little or no interaction with an end-user. Therefore, a request to change network providers (change network profile on a SIM) doesn't need to come from a device. Instead, the connectivity can be managed and authorized remotely by the service provider. This rationale led to the M2M RSP solution to be conceived and operated on a profile 'push' model, as represented below:

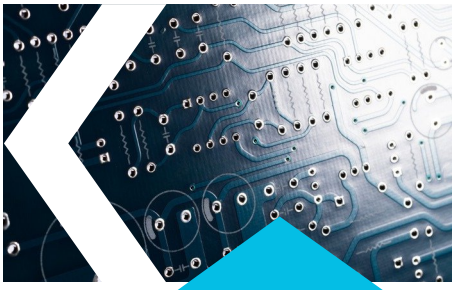


M2M RSP-push process

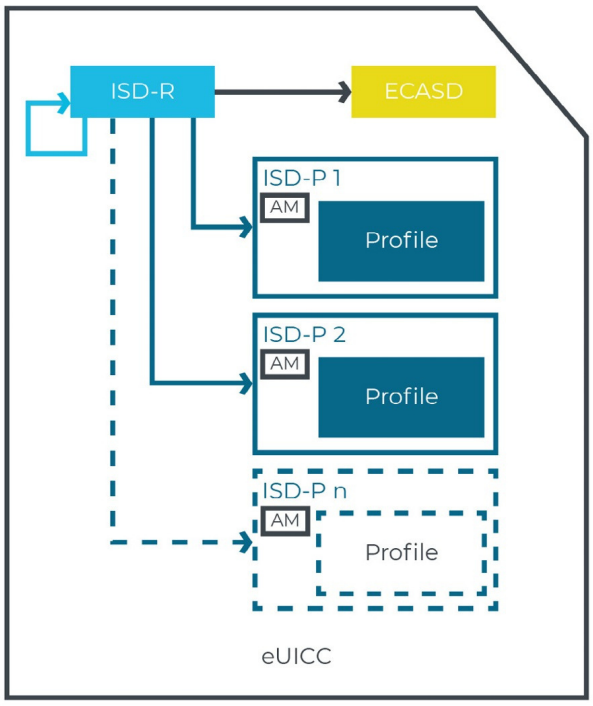
The RSP architecture is based on the existing SIM functionality (as defined by ETSI) and the smartcard security domain concepts of GlobalPlatform. These allow the eUICC to operate akin to a standard SIM whilst affording RSP management from the off-card entity: the remote provisioning server.

The eUICC security domain architecture comprises the following elements:

- The eUICC Controlling Authority Security Domain (ECASD) represents the offcard entity Certificate Issuer (CI).
- The Issuer Security Domain – Root (ISD-R) represents the off-card entity Subscription Manager – Secure Routing (SM-SR).
- The Issuer Security Domain – Profile (ISD-P) hosts a profile, representing the off-card entity Subscription Manager – Data Preparation (SM-DP).



See our essential guide to GSMA eSIM certification for more information on how certificates are obtained.



Security domain architecture overview

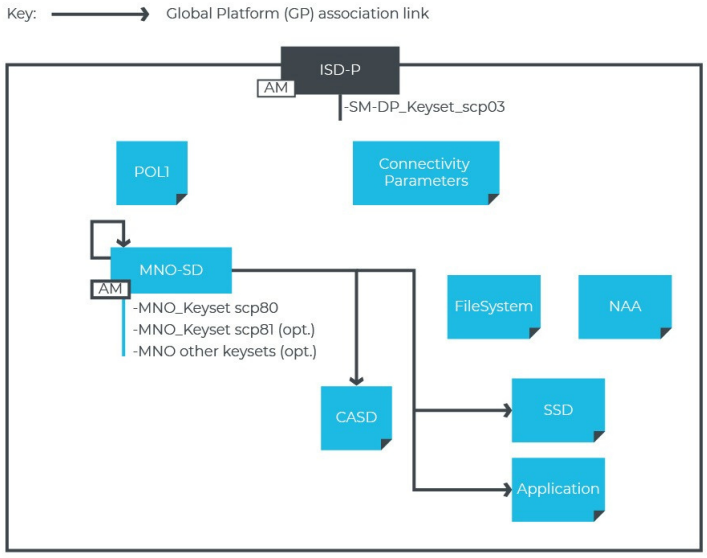
The ECASD is installed by the EUM in the process called personalization. The ECASD contains a unique eUICC-ID (EID) including embedded codes for country, issuer, and unit identification. The EUM also installs a certificate for authentication, a public key for verifying certificate signatures and a private key for elliptic curve cryptography.

The ISD-R is also installed by the eUICC manufacturer. The ECASD associates with the ISD-R, which is the only component with visibility and access to an

ISD-P. Upon strict conditions (and upon instruction), the ISD-R also creates, enables, disables, and deletes ISD-Ps, and provides functions for secure channel setup between the SM-DP and the ISD-P. It is also able to instigate profile fallback if a fallback profile is available. Fallback is where a disabled profile is enabled automatically if connectivity isn't possible on the enabled profile.

Only one ISD-P may be enabled at any time. An ISD-P contains profile components specified by and under the full control of the network operator.

The primary component of a profile is the MNO-SD, representing the network operator with their over-the-air key sets. Other components are the configurations to support use of Network Access Applications (NAA), supplementary security domains (shown as SSD), policy rules (shown as POL1 in diagram overleaf) and connectivity parameters.



Profile structure overview

M2M RSP uses a push model with a server provisioning and managing these profiles, in three phases:

- The SM-DP protects and stores profiles on the server in readiness for allocation, secure download and installation onto the target eUICC.
- The SM-SR ensures the secure transport of both eUICC platform and profile management commands in order to load, enable, disable and delete profiles on the eUICC. It communicates with the target eUICC using secure messaging (SMS) encrypted with its ISD-R pre-shared keys. This message invokes the eUICC to establish a secure data communication session

(HTTPS) back to the SM-SR. The eUICC may also trigger itself to establish an HTTPS session.

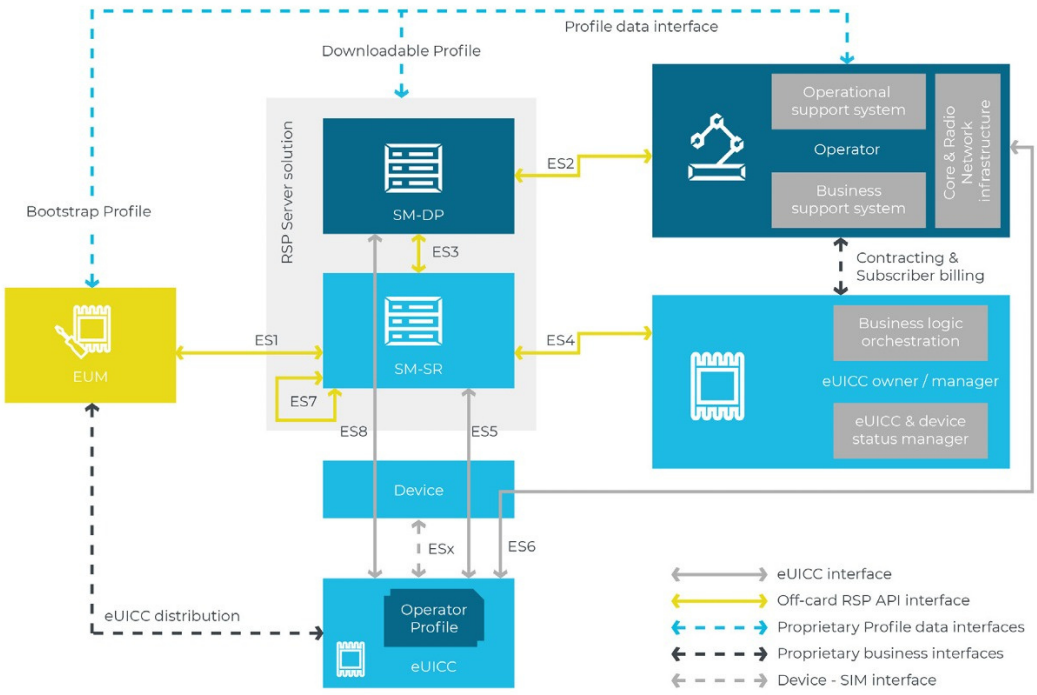
- The SM-SR uses its ability to manage the ISD-R to facilitate secure download and installation of the selected encrypted profile from the SM-DP into a newly created ISD-P. This secure communication establishment also allows the SM-SR to manage the eUICC and its installed profiles.

End-to-end security is built into RSP. All exchanges between the SM-DP, SM-SR, and eUICC rely on digital certificates (PKIs) or pre-shared keys (PSKs), which can be revoked at any time if security concerns arise. An eUICC receiving SMS messages uses AES encryption, and HTTPS card to server data sessions use Transport Layer Security (TLS) to protect over-the-air communication.

It is worth noting that the M2M RSP architecture ecosystem is only part of the overall eSIM and profile management picture, as the SM-DP and SM-SR effectively act on behalf of the eSIM and/or profile owners. These have their own business and operational systems that enforce and govern the following:

- Which profile should be selected,
- Why and when a profile should be deployed,
- The target eUICC.

These business and operational systems perform their roles and instruct the RSP platforms through well-defined integration interfaces (ES2 & ES4), using standardized APIs.



M2M RSP architecture

Onboarding an eSIM-enabled device into the M2M RSP ecosystem for eSIM and remote profile management first requires the uploading of information about the eSIMs, also referred to as the eUICC information set (EIS), onto the SM-SR. This is executed using a standardized API, known as registerEIS, via the ES1 interface. The information set includes the eUICCs management keys. Should the eUICC owner need to change its managing SM-SR platform, an SM-SR swap procedure is defined to facilitate this handover via the ES7 interface. Additionally, the eUICC owner may need to load the identity of the device and its eSIM ID (EID) into their own business logic engine to orchestrate the business rules which drive the eSIM and profile management events.

In order to provide initial connectivity to the device and allow for the initial remote eUICC management, a bootstrap profile is loaded onto the eUICC, at the point of manufacture, by the EUM. Selection and delivery of the bootstrap profile to the EUM is a commercial and business engagement, as well as a technical interaction, all of which are out of scope of the RSP specification.

Downloadable profiles also need to be sourced and loaded into the SM-DP in readiness for post deployment profile management events. Again, selection of the supplying operator, generation and delivery of these profiles to the SM-DP provider/platform are out of scope of the specification, however, these digital artifacts must conform to the specified format.

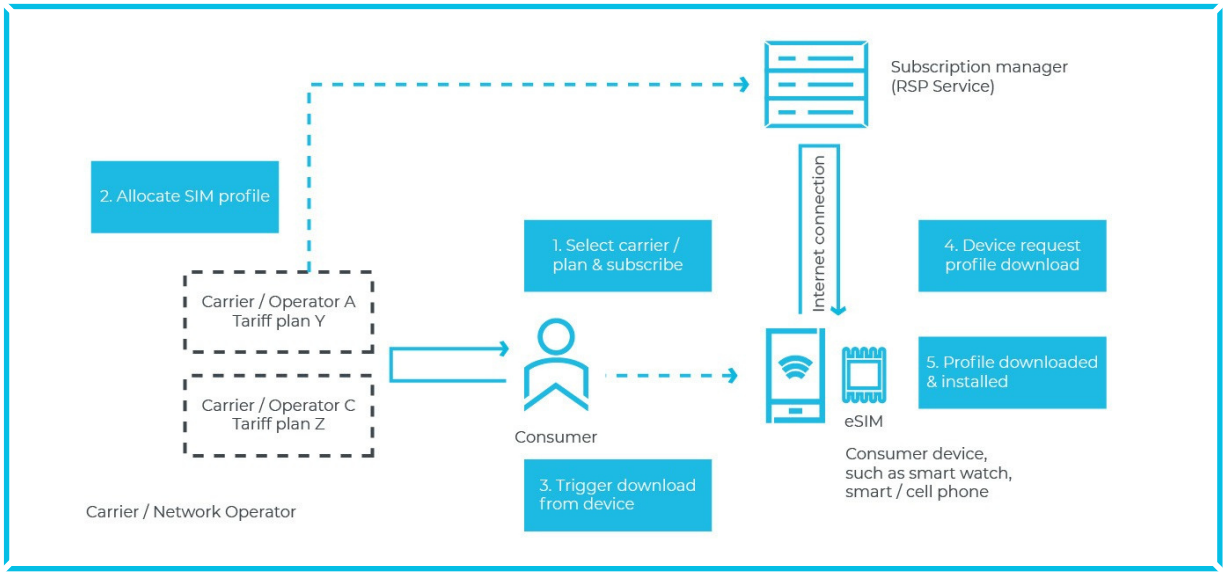
The M2M RSP architecture and specification allows for business model flexibility. It can support deployment scenarios where the entire ecosystem is under the management of the mobile network operator. It can also support a split responsibility where the SM-DP is managed by the network operator, as the profile owner, and the SM-SR is under the control of another entity, which owns and manages the eUICC or the device.

For the full GSMA M2M RSP solution specification, visit: **www.gsma.com/esim/resources/sgp-02-v4-1-pdf**

Consumer pull: users request RSP

GSMA released the first iteration of the consumer RSP solution in 2016, developed for handling consumer device provisioning scenarios. The primary target is network operators serving companion devices such as wearables, with smartphone support covered in the next iteration. Its basis is an eUICC element, with many security and communication concepts that are similar to M2M.

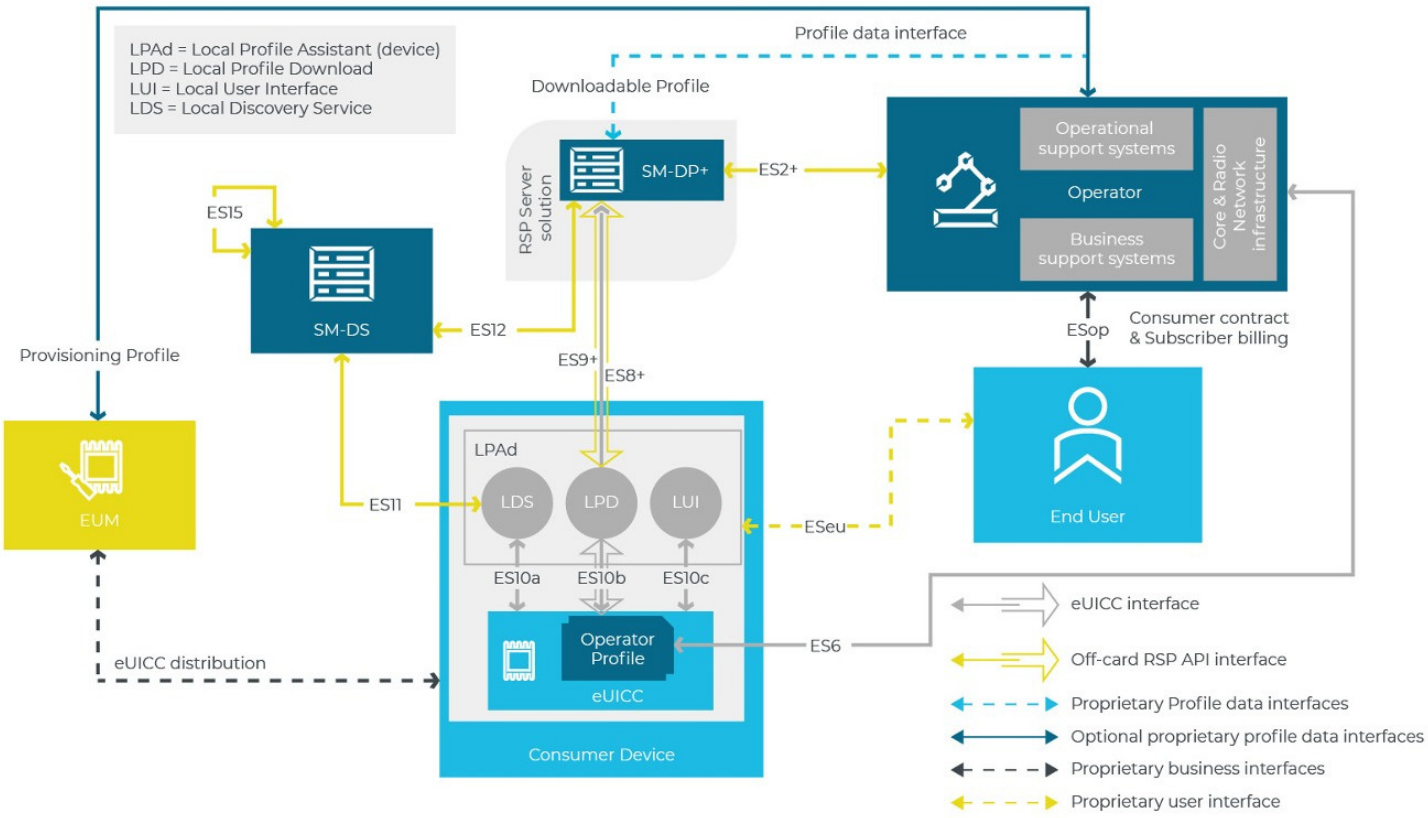
The biggest difference in the consumer RSP solution is its use of a pull model instead of the push model of the M2M solution.



Consumer RSP-pull process

The consumer solution has four elements:

- The SM-DP+ prepares, downloads and manages profiles onto the eUICC, and protects credentials on the server. It effectively combines the SM-DP and SM-SR functions in the M2M solution.
- The Local Profile Assistant (LPA) provides local eUICC profile management and functions for user interface integration for end user profile downloads and management tasks.
- The SM-DS allows an eUICC to establish if and on which SM-DP+ a profile has been allocated for it. The use of the SM-DS by the profile issuer to publish profile availability is optional.
- The eUICC has modifications supporting the LPA for end user interaction.



Consumer RSP architecture

In the consumer arena, the cellular device owner is usually also the subscriber to the network, being named on the billing account. Obtaining a new profile for an eSIM-enabled device will require the necessary interaction with a network operator to register for a new account or prove you're the account holder. The network operator will then establish that you intend to use an eSIM device and need a downloadable profile, after which they will place this on the download server (SM-DP+) and guide you how to use the device to trigger the download, installation and enablement of the profile.

This process could be repeated to add other profiles into the eSIM so that you can get service from a different network operator for use when travelling, for example. Profile changes have to be triggered by the consumer. The adding or enabling of new profiles may not always be possible if the initial operator profile or device is set to only allow the use of one network.

Unlike the M2M solution, which allows connection to one server only, the consumer solution allows connection of any eUICC and SM-DP+ as long as they share the same root PKI certificate. A consumer solution is technically different from an M2M solution and there are clear technical barriers that prevent one from acting as the other and vice versa. However, introducing adaptations which mean that the same overall architecture is capable of serving both scenarios is not infeasible; it is a matter of design and addons.

For the full GSMA Consumer RSP solution specification, visit: **www.gsma.com/esim/resources/sgp-22-v2-2-2**

M2M RSP use cases

Innovation around the M2M RSP solution is enabling many exciting use cases.

Agriculture
Corporate farming is often spread across states and countries, creating a need for centralized network management. RSP lets agriculture firms deploy the same eSIM-enabled devices, then choose a network provider best suited for service in each location.

Automotive
Rather than outsourcing connectivity to one network operator, automakers can handle eSIMs in their vehicles as a managed service with RSP. With emerging cellular vehicle-to-everything (CV2X) applications, RSP also underpins the provision of cellular connectivity which enables better service for owners when buying or selling vehicles and registering or de-registering services.

Home security
With eSIM technology, one home security hub configuration can be delivered anywhere and provisioned remotely by the monitoring service. If a change of network provider is required due to commercial reasons, the hub is easily re-provisioned in another network.

Item tracking
Corporations also often have locations in more than one city. One type of eSIM-enabled item tracking device can be used everywhere, managed via RSP, which can change profiles and serving network if an item moves to another location where its original network has no coverage.

Shipping and logistics
Knowing the exact location of goods in real-time is essential. With RSP, eSIM-enabled tracked assets can be shipped anywhere and have their connectivity assured by the ability to remotely deploy a profile for any network across the world, without swapping SIM cards before or during transit.

Smart energy
Instead of building their own mesh network infrastructure, a utility company can deploy an eSIMenabled smart energy device anywhere within cellular coverage. With RSP, utility companies can change networks remotely, reducing the complexity and cost of managing cellular devices. With scalable connectivity, they can maximize the benefits of real-time consumption/ generation data and provide multiple customer benefits, such as realtime billing.

Wearables
M2M use cases cover loan devices, and where issuers - not users - choose network providers. Medical and industrial devices such as glucose monitors, electrocardiogram (EKG) monitors, fall detectors, AR glasses, voice search hearables, and others are great cases where RSP can help manage devices. Replacing conventional SIM cards with eSIM technology also helps make these devices smaller and more tamper resistant.

M2M RSP streamlines IoT deployment

RSP and eSIM technology are huge breakthroughs, relieving a major bottleneck in at-scale device deployment for the IoT. A growing ecosystem is discovering RSP benefits for more use cases. Ample innovation opportunities exist for established firms and startups who can build on the proven value of RSP solutions available now.

With security as a given, the biggest benefit of RSP is streamlined deployment. New cellular connectivity specifications including LTE-M and NB-IoT, supported by device chipsets and intellectual property for custom designs, are gaining momentum rapidly. The coming challenge for enterprises, MNOs and IoT service operators will be activating millions more devices quickly and securely.

- MNOs can offer unique M2M and IoT services without adding human-intensive processes, choosing instead to use proven M2M RSP solutions. The integrity of their network is always protected as eSIM technology is just as secure as tried-and-trusted conventional SIM card technology. Supporting M2M RSP expands their customer base and allows them to capitalize on the IoT growth.
- Device makers choosing cellular connectivity can distribute their devices to customers worldwide, anywhere cellular coverage exists, with one certified eSIM-enabled device. Costs are reduced as the need to stock and manage many variants of SIM cards is eliminated.
- Enterprises can use RSP to virtually manage a secure array of devices deployed across geographic regions. Devices and customers can be onboarded and offboarded easily from a unified RSP management scheme. Product upgrades and new services can be provided remotely, supporting innovation and service differentiation.

Moving IoT applications from pilot to small-scale to large-scale hinges on dependable, secure interoperability for devices across networks. The GSMA specifications and certification processes foster end-to-end trust and worry-free interoperability.

Integrating M2M RSP

Ideally, an M2M RSP solution would integrate with existing subscriber management solutions and customer service tools. If RSP can be managed within existing MNO workflows, servicing eSIM technology alongside existing SIM card technology is simple.

Kigen Server Solutions are designed with that simplicity in mind. Kigen RSP Service provides a GSMA-compliant RSP implementation focused on the M2M solution. Kigen is certified via audit as an SAS-SM provider for SM-DP and SM-SR capability.

For integration, Kigen Server Solutions have REST/SOAP APIs. Existing provisioning and management applications can access RSP Server through callable functions.

Kigen is also breaking ground in eUICC implementations for device makers. Kigen OS is a low-footprint software stack enabling integration of SIM functionality into SoC designs. The target can be either an embedded SIM on a discrete hardware package or an integrated SIM (iSIM) within a secure enclave running on-chip in an SoC.

Find out more about
Kigen SIM solutions, visit:
www.kigen.com

Kigen