


Remote eSIM Provisioning Cookbook



How to build your own
eSIM Management Service

Table of Contents

Your Kitchen – Your Rules

Why you would host your own eSIM RSP Service (Remote SIM Provisioning)

What took eSIM so long – and why it will succeed anyway

Flavours of eSIM

Managing eSIM for consumer devices with SM-DP+

Managing eSIM for M2M devices with SM-DP and SM-SR

Best of two worlds – introducing SM-DP+ for IoT devices

Indispensable Ingredients

Infrastructure – moving to cloud

RSP Software – microservices & containers

System Utilities – embracing open source

GSMA System Certificates – gatekeepers of the ecosystem

The MNO Profile – virtualisation of the SIM

The Master Recipe

Turn on the heat – putting the infrastructure in place

Stir until combined – deploying the RSP system

Season to taste – integrating systems and processes

Inspecting the kitchen – the GSMA security audit

Ready to serve – going live with the production system

Before you begin – well planned is a success half done

Every great Kitchen has a great Team

Why achelos is the right partner for your RSP service

Where we are coming from

What drives us beyond our enthusiasm for technology

Annex

Abbreviations

References

Your Kitchen – Your Rules

Why you would host your own eSIM RSP Service (Remote eSIM Provisioning)

eSIM – the digital transformation of the plastic SIM – is speeding up. As adoption is set to scale globally from millions to billions, the use cases for players in the mobile telecom market to become an enabler of this game changing technology take on new urgency:

- Infrastructure Providers – extending their solution stack with eSIM Management
- Service Providers – adding eSIM Management to their service offering
- Mobile Network Operators – managing eSIM subscriptions in-network

Although “eSIM-Management-as-a-Service” has been available for years from established SIM vendors, companies that deliver RSP services to their customers will need, in the long-term, commercial and technical independence to offer competitive products and services. And Mobile Network Operators (MNO) can have compelling reasons to fully control storage and processing of subscriber data “in-network”.

One alternative to the Software-as-a-Service model - developing the RSP software - is a huge project that demands deep knowledge of the embedded security domain and substantial development resources. The second alternative - using “off-the-shelf” RSP software - eliminates the cost and risks of a development project and instead focusses efforts on building an RSP service that perfectly fits the business demands.

achelos offers a complete suite of RSP solutions covering the components specified by the GSMA (GSM Association) as well as solutions that go beyond the specified standards. As a software house we not only develop customised features and extensions for all products but also fully bespoke solutions.

To the challengers of the eSIM Management status quo, we deliver control:

- Control of infrastructure and system configuration
- Control of quality and costs
- Control of regulatory compliance
- Control of customer data retention
- Control of integration with systems and processes
- Control of customisation for a unique offering

With the “RSP Cookbook” we give a detailed overview to help you determine which approach is right for you, “RSP-as-a-Service” or “Do-It-Yourself-RSP”. You will find information about the essential ingredients and, with a step-by-step recipe, how you can build an RSP service that you fully control and that is enabling your business strategy in the long-term.

What took eSIM so long – and why it will succeed anyway

Since the introduction of eSIM technology most known eSIM Management solutions, better known as Remote SIM Provisioning (RSP), have been offered as a service. It was, and largely still is, seen as an evolution of the traditional plastic SIM card business,

inextricably linked to the manufacturing process of the secure hardware chip. The only difference being that the Mobile Network Operator (MNO) buys a "virtual" SIM instead of a physical one. However, the concept of eSIM actually enables very different models.

eSIM is separating the non-reprogrammable SIM chip from the MNO profile and transforms the profile into a truly digital asset. It becomes remotely manageable based on a purpose-built secure element, the eSIM chip. While the SIM was designed to be removable, the eSIM chip is a fixed component of the device with the capacity to store multiple MNO profiles.

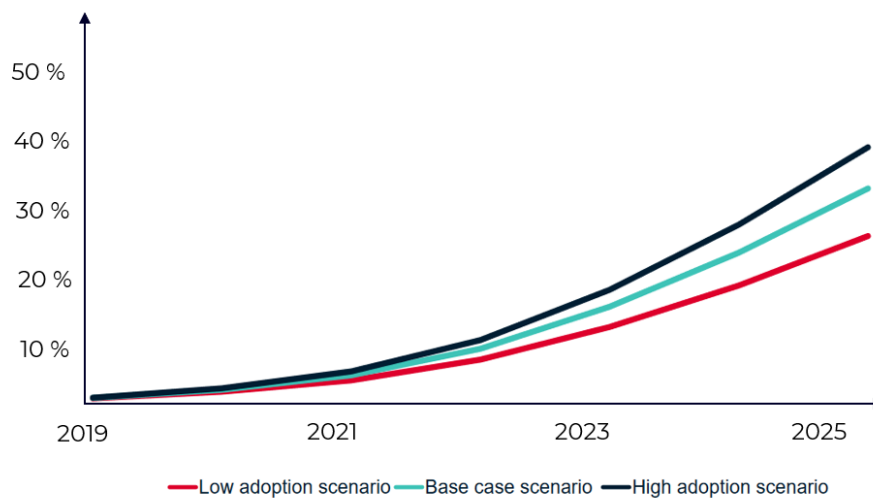
Despite the obvious advantages of this approach, uptake of the technology has been slow. Mobile operators were sceptical to give their customers an easy way to “churn” and to sign up with competitors instantly by simply using an app on their mobiles. On the other

hand, device manufacturers (OEM) were hesitant to increase their Bill of Materials, especially for low-cost devices, which would add a functionality that was neither understood nor demanded by customers. It created a chicken and egg situation that stalled the

adoption of eSIM for years, leading to very limited usage where “eSIM Management-as-a-Service” from established manufacturers was the only option available and viable. Times are changing, however, and fast, as you would expect from a disruptive digital technology. There is now no doubt throughout the industry that eSIM will largely replace the SIM in the not too distant future. 5G created significant momentum. Since its launch the major OEMs have been releasing an expanding range of 5G

devices supporting eSIM. Mobile Network Operators have started to view eSIM as an opportunity to strengthen the customer relationship rather than as a threat to it. These developments are reflected in the latest numbers from GSMA itself, the global Association of Mobile Network Operators, that estimate eSIM connections to reach between 1.9 and 2.8 billion connections, the equivalent of 26%-40% of total market share, until 2025 alone.

eSIM smartphone connections as % of total smartphone connections



Source: GSMA

In line with this forecast a growing amount of industry news is emerging, such as a Tier 1 MNO in Europe that will make eSIM the default subscription activation process and rumours that one of the leading mobile phone manufacturers is about to introduce “eSIM-only” models without the space consuming SIM slot. Besides the projected growth of eSIM usage, there is another major development that makes the operation of RSP

services a lot more efficient – **cloud**. Until very recently the traditional RSP service setup demanded substantial on-premise infrastructure within a certified high-security area. For innovative newcomers the entry barriers were largely too steep to surmount. Cloud, especially the GSMA security-certified, public cloud offered by MS Azure and AWS across multiple sites and regions, has changed the game fundamentally. It reduces costs

substantially while offering scalability combined with telco-grade reliability, enabling companies to host an RSP service that

effortlessly expands in step with increasing demand.

Flavours of eSIM

GSMA have defined three different eSIM architectures. Initial demand came from the M2M industry and led to the SGP.01 standard for M2M devices in 2013. The standard SGP.21 for consumer devices was released in 2015. The latest standard SGP.31 for IoT devices was published in 2022, addressing shortcomings of the initial M2M standard. In the following chapters we show a brief overview of each architecture.

Managing eSIM for consumer devices with SM-DP+

The consumer architecture (SGP.21) follows a client-driven pull model that gives control over remote provisioning and local management of the profile to user of the device. The solution consists of the SM-DP+ (Subscription Manager Data Preparation plus) for the creation and protection of MNO profiles and a specific application on the device, the LPA (Local

Profile Assistant) that manages the communication between eSIM and backend. The optional SM-DS (Subscription Manager Discovery Server) enables automated profile discovery, if selected as an activation method by the Mobile Network Operator.



SGP.21 eSIM Architecture for Consumer

Managing eSIM for M2M devices with SM-DP and SM-SR

The GSMA M2M architecture (SGP.01) is a server-driven push model that enables the centralised management of eSIM devices and profiles and involves two system components. The SM-DP (Subscription Manager Data Preparation) represents the profile owner and manages the download of MNO profiles. It securely encrypts the network access credentials (i.e., the profile) and manages the remote provisioning process.

The SM-SR (Subscription Manager Secure Routing) oversees eSIM management and represents the eSIM device owner. It is also the entity that securely delivers the encrypted MNO profile to the eSIM and manages it remotely over its lifetime using a specific set of operations, such as profile activation, deactivation and deletion.

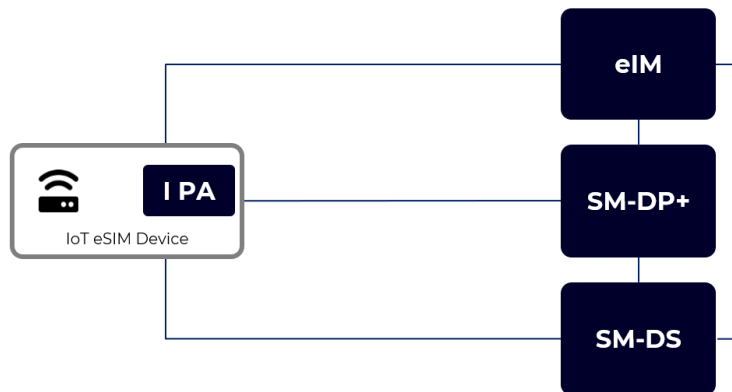


SGP.01 eSIM Architecture for M2M

Best of two worlds – introducing SM-DP+ for IoT devices

The architecture designed by GSMA for M2M (SGP.01) often creates difficult commercial scenarios that stand in the way of effective integration. For example, the SM-SR as the lifecycle manager of an eSIM, needs to integrate with SM-DPs of various MNOs before their profiles can be made available. It can make deployment and operation of a GSMA-compliant RSP system for M2M complex and expensive, contributing considerably to its low uptake within the cost sensitive IoT ecosystem.

In addition, the M2M specification requires SMS and HTTPS communication protocols that have compatibility issues with popular IoT technologies like NB-IoT and LPWA, which usually demand IoT-specific light weight protocols for maximum energy efficiency. The need to overcome these limitations as well as the much greater success of the Consumer RSP specification have driven GSMA to create the SGP.31 standard that defines the following architecture:



SGP.31 eSIM Architecture for IoT

While relying on the market-proven components SM-DP+ and SM-DS, SGP.31 introduces a new component in the RSP architecture, the eIM (eSIM IoT remote Manager). It manages the eSIM and profile states remotely, including initiation of profile download requests directly from SM-DP+ or via SM-DS. Additionally, the eIM can take the role of a protocol converter for network constrained devices that do not support HTTPS communication and eSIM devices can be easily associated with different eIMs over their lifetime. As in the consumer solution, a special application is required on the device to

manage the communication between eSIM and backend. This is the IPA (IoT Profile Assistant), with the capability to manage the eSIM using a remote system instead of a human user as the major difference to the consumer architecture.

Although there is no doubt that the initial M2M standard will remain available for the foreseeable future, not least due to a significant amount of legacy deployments, it seems equally clear that the future of cellular IoT connectivity will be managed along the principles described in this new standard.

Indispensable Ingredients

If you want to decide whether hosting your own RSP will be beneficial to your business, you need to have a clear understanding of what this entails. Within this chapter we describe the core components required to establish an efficient RSP service that puts you in control.

Infrastructure – moving to cloud

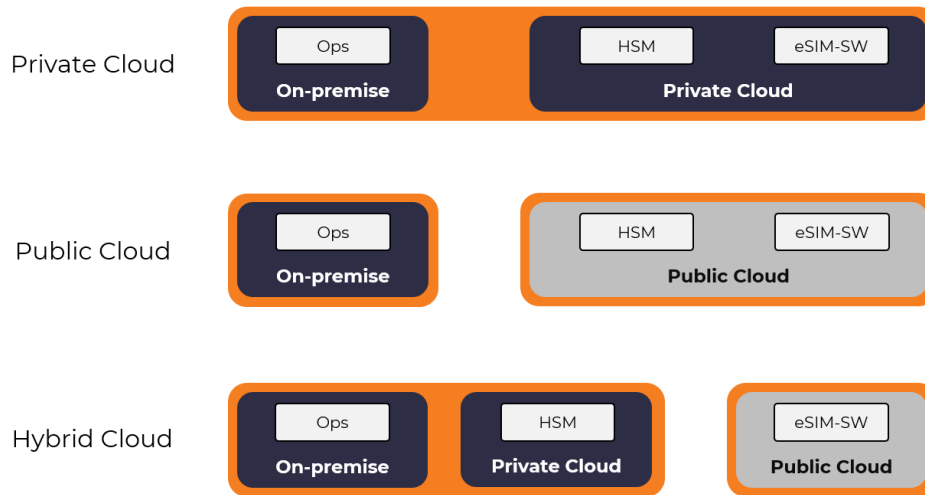
Before Service Providers can offer eSIM RSP services they must perform an audit according to the GSMA's Security Accreditation Scheme (SAS-SM). This shall ensure that the service is provided in accordance with the security expectations of GSMA's members from the global Mobile Network Operator community. Compared to solutions that are outside GSMA's accreditation scheme, SAS-SM adds

a significant layer of complexity concerning infrastructure. Yes, you can build your own infrastructure, buying hardware for processing power, memory, data storage and the like, renting a secure site and hiring expert staff. But even if you already have your own datacentre in place, chances are you have started to plan the migration to the cloud. Why? Because cloud focuses on delivering:

- **Cost savings** - eliminating capital expense of buying hardware and software and reducing operational expense of running an on-site datacentre
- **Scalability** - getting the right amount of resources when needed from the geographic location where needed
- **Reliability** - mirroring data at multiple redundant sites on the cloud provider's secured network for data backup and disaster recovery

The following diagram shows the deployment options with respect to the three key components of an RSP solution:

- Ops: operations terminal for administrative access
- RSP-SW: eSIM management application
- HSM: High-Security-Module protecting key material in purpose-built hardware



Main RSP Cloud Deployment Options

Private Cloud maintains services and infrastructure on a private network and is exclusively used by a single organization. It can be located on-premise or hosted by a third-party service provider. SAS-SM security certification must be performed for both sites under the single responsibility of the RSP service owner.

Public Cloud is owned and operated by third-party service providers delivering their computing resources over the Internet to

multiple tenants. Google Cloud, IBM Cloud, Microsoft Azure and Amazon Web Services (AWS) are examples of public cloud. The latter two offer SAS-SM certified datacentres in specific regions and are therefore ideally positioned to host RSP solutions.

Hybrid Cloud allows data and applications to be split between private and public cloud, which might be required in specific cases to utilise existing infrastructure or to comply with data sovereignty regulation.

RSP Software – microservices & containers

Applications were traditionally built as monolithic pieces of software. Monolithic applications have long life cycles, are updated infrequently and changes usually affect the entire application. Adding new features requires reconfiguring and updating the entire stack, from communications to security. This

costly and cumbersome process delays time-to-market and updates in application development. Modern software, especially for high performance applications within the telco sphere, should be designed based on a microservices architecture and packaged in containers to avoid these pitfalls.

Microservices is an architectural concept for building a distributed application. They break an application into independent, loosely-coupled, individually deployable services. This architecture allows for each service to scale or update using the deployment of service proxies without disrupting other services in the application and enables the rapid, frequent and reliable delivery of large, complex applications.

Containers are a lightweight and efficient way for applications to move between environments and run independently. Everything needed to run the application, except for the shared operating system on the server, is packaged inside the container object: code, run-time environment, system tools, libraries and dependencies. There are substantial benefits of these two concepts that include:

- **Resilience**, so an application still functions if a part of it goes down because microservices allow for quickly deploying a replacement
- **Scalability**, by meeting demand more efficiently when microservices only scale the necessary components
- **Lifecycle automation**, with individual components of microservices that easily fit into continuous delivery pipelines

System Utilities – embracing open source

It's not that long ago that open source was called into question for business environments but that has changed profoundly, instead transforming into a vital enabler of large scale systems.

To host an efficient, light-weight RSP solution it is important to select tools that are well known throughout the industry and have strong communities.

Below are some of the tools we love to work with:

- Docker: a set of tools for building and running software in containers
- Kubernetes: an orchestration tool for managing your applications running in containers
- PostgreSQL: also known as Postgres, is a free and open-source relational database management system (RDBMS) emphasizing extensibility and SQL compliance

- Prometheus: a monitoring and alerting toolkit. It consists of a time-series database and some tools to collect metrics from applications or servers
- Grafana: a dashboarding tool. Grafana lets you create visual dashboards from data stored in different places, including Prometheus
- Elasticsearch: a search engine which to analyse log files and often combined with Logstash and Kibana to gather logs from servers and applications; when these three tools are combined it's called the "ELK stack"
- Nginx: an open-source web application server targeting multi-language microservices-based applications

GSMA System Certificates – gatekeepers of the ecosystem

We mentioned this before but due to its significance, it's worth repeating. Before a company that is hosting its own RSP system

can offer the service, it must perform a security audit according to the GSMA's Security Accreditation Scheme (SAS-SM).

In the words of GSMA, *"the Security Accreditation Scheme (SAS) enables mobile operators, regardless of their resources or experience, to assess the security of their SIM and eSIM suppliers, and of their eSIM subscription management service providers"*.

Only after the successful audit a company will be able to request the signed system certificates that are required for the RSP service to interact with the open eSIM ecosystem. This setup reflects the belief that eSIM services will always be provided by established manufacturers to the MNO community in a continuation of the existing SIM business model. However, this is far from a certainty. With infrastructure moving to the cloud and large-scale adoption of eSIM as the preferred subscription lifecycle management mechanism, the case to host an RSP service is getting continuously stronger not only for

Infrastructure and Service Providers, but for Mobile Network Operators themselves as well.

While the SAS-SM audit - by definition a supplier accreditation procedure - is a reasonable requirement for external providers that are offering their products and services to MNOs, it is less clear what its benefit would be for Mobile Network Operators that want to host the RSP service in-network. This makes it in our view likely that those Mobile Network Operators will be able to receive the RSP system certificates either without or a light version of the SAS-SM audit.

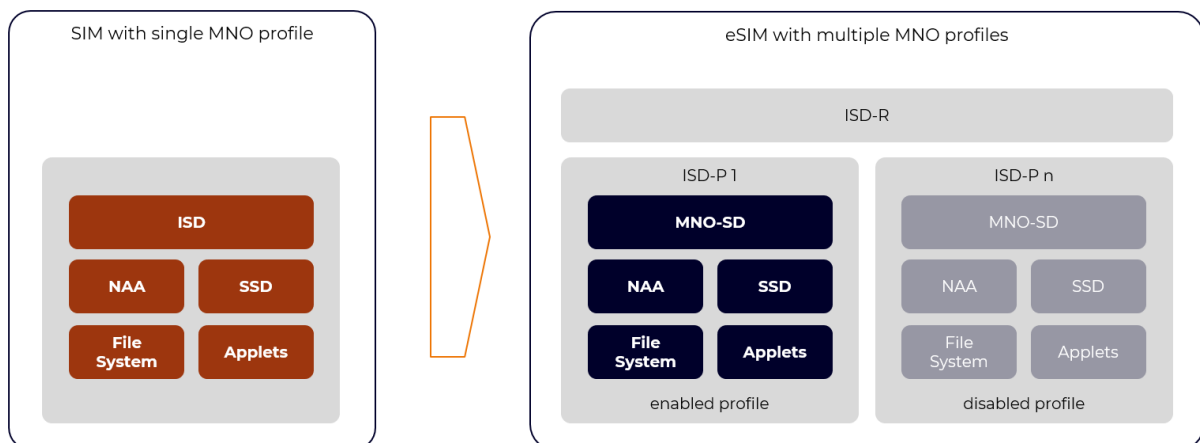
The MNO Profile – virtualisation of the SIM

The core functionality of the operator profile, from inception of the first digital mobile standard GSM to the current 5G releases, is the storage of subscriber credentials and the implementation of algorithms and applications used for network access authentication. Its role in the 3GPP Authentication and Key

Agreement (AKA) remains a key feature of cellular mobile network security and has not changed with the introduction of eSIM, other than adding the capability to load several profiles onto a single chip and manage them remotely.

To accomplish remote profile provisioning and management in a high-security manner, on par with existing SIM manufacturing processes, three new types of Security Domains have been introduced to the eSIM architecture:

- **ISD-R**: root security domain managing the state of all profiles
- **ISD-P**: profile security domain created for each profile during provisioning
- **ECASD**: crypto security domain for key establishment and authentication services



SIM vs. eSIM

The MNO profile, that is provisioned into eSIM, includes the following components:

- **MNO-SD** (MNO Security Domain): managing applications in the profile on behalf of the MNO, performing the same function as ISD (Issuer Security Domain) on SIM
- **NAA** (Network Access Application): such as SIM and USIM, which are selected by the device to access the related mobile network

- **File System:** containing data files that store subscriber and network information
- **Applets** (optional): programs for additional functions the MNO may want to execute within the profile, for example steering of preferred roaming partners

To guarantee that MNO profiles can work across various provider systems, the industry agreed to use a standardised description of its content. MNO profiles for eSIM have to comply with the format defined in the “Interoperable Profile Package Description” specification of the Trusted Connectivity Alliance (TCA), formerly known as SIM Alliance.

Because the profile was an indivisible element of the plastic SIM it usually was developed by SIM manufacturers as part of the SIM contract. Few companies were able to insert themselves into the value-chain and offer independent profile development capabilities. This inefficiency came at a price - with the ubiquitous use of smartphones a great deal of functionality moved to the device, especially related to personal subscriber data. Consequently, there are now few applications which add substantial value when placed

within the profile, rather than the device. Just one example is the complex phonebook structure often defined within MNO profiles, taking up half its memory, even though smartphones manage this function anyway much more conveniently.

Again, eSIM is changing the landscape by breaking the plastic SIM's bond between digital profile and chip hardware and with it the deep-rooted incentives for the inclusion of avoidable, but memory demanding functions. A new breed of specialised companies with expert domain knowledge in telecom embedded technology is coming to market, that offer MNO profile development, either as a service or through open-market tools. It is not only much more efficient but also provides the Mobile Network Operator the complete ownership of its own profiles.

The Master Recipe

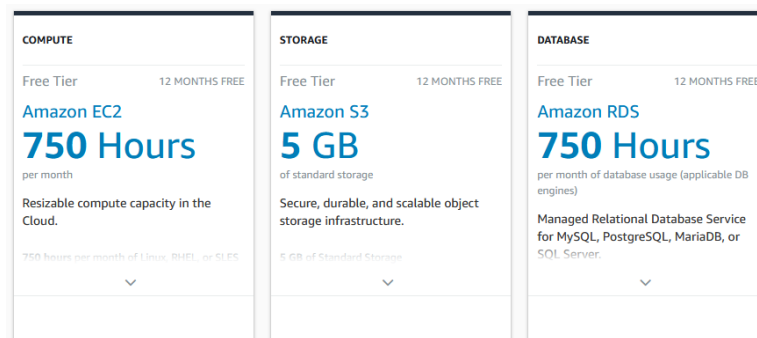
Now that you know about the ingredients of an RSP solution, let's look at the tasks required to build a scalable, flexible and reliable RSP service for eSIM management.

Turn on the heat – putting the infrastructure in place

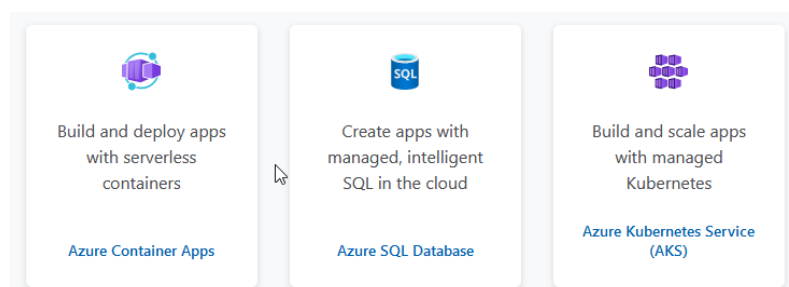
This is where it starts and becomes only as complicated as you need it to be.

Even a light-weight RSP software needs servers, racks, an HSM, storage and power back-up, as well as firewalls, backup tools and the like. All this must be installed in a secure site with things like CCTV, access control

readers, fire and water protection equipment and so forth. Alternatively, you create an account with an SAS-SM certified public cloud provider like Amazon AWS or Microsoft Azure and order on-demand services with a couple of clicks, spinning up your infrastructure near instantly.



AWS Web Console

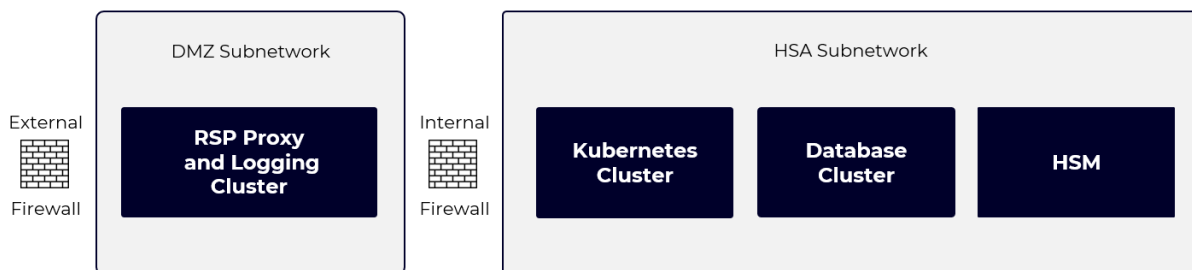


MS Azure Web Console

Stir until combined – deploying the RSP system

Once the infrastructure is in place, you can start deploying the RSP staging system. This pre-production system is crucial for the lifetime of the RSP service since it remains accessible to your RSP software provider who will play a key role during deployment and service operation. The system fulfils vital functions

during release testing and incident resolution but also for the initial SAS-SM audit before you have received the signed certificates for the final production system. The architecture diagram below will vary depending on the service configuration that you decide to build.



RSP Service Architecture

The system requires the configuration of the following components:

- Container Registry (Docker container storage)
- Kubernetes Cluster (RSP Application cluster)
- Worker Nodes for Kubernetes cluster (Virtual Machines)
- Proxy Nodes (Virtual Machines)
- Database Services
- HSM (High Security Module)
- Firewalls

Cluster management nodes are responsible for the entire cluster health and perform orchestration of all running services. The logging cluster can host Elasticsearch nodes to store system logs and provides access for the log monitoring software.

The HSM must be FIPS 140-2 level 3 certified (a standard required in many regulated

industries that store and transfer sensitive information such as Banking, Health and Government institutions).

The RSP software is deployed in the form of containers in the virtual environment managed by the container management software. For the deployment to be performed efficiently, the right design of the software is essential.

This is hard to judge from outside the code and requires a software provider experienced with state-of-the-art cloud development and deployment practises. The following major elements should be covered.

The software should be light-weight with a small application footprint, designed to have small memory and CPU usage, and a low usage of system resources in general. To achieve this, the software must avoid code bloat and have optimised algorithm efficiency. Rather than a one-time effort, this requires the right design from the start and continuous optimisation over all releases of the software.

Second, the software should be developed according to Continuous Integration (CI) principles. CI avoids the long release cycles of traditional software development practices. These are prone to a high risk of errors arising without developers noticing them, which makes it near impossible to correct them quickly and can lead to severe, prolonged service disruption.

Not least, as the final GSMA-certified production environment will be only accessible to your Ops team, you will want the software deployment process to be as straight forward and reliable as possible.

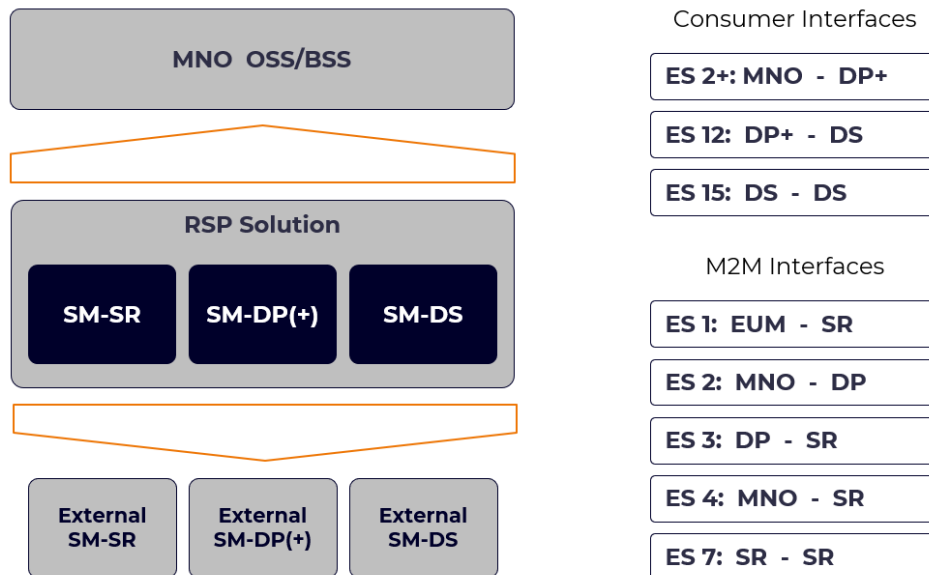
To achieve this, make sure your RSP software provider is following these principles:

- Staging System as a cloned, scalable version of the production environment to avoid failures due to significant differences
- Version Control to maintain a code repository
- Build Automation for source code compilation
- Self-testing to confirm - once the code is built - that it behaves as expected
- Test Cases that reproduce every identified bug
- Fast & secure delivery making builds readily available to your Ops team

Season to taste – integrating systems and processes

After the RSP solution is deployed, it is time to look at how service functions can be exposed to other systems. Each RSP deployment will have different requirements depending on the

target service. GSMA has specified several interfaces to ensure all components within the eSIM ecosystem can exchange information in an interoperable, standardised way.



RSP Solution Integration and Interfaces

The scope of integration for the consumer solution is rather simple:

- ES2+ interface is used by the MNO to order profile downloads and to receive operation notifications
- ES12 and ES15 interfaces allow a device the automated discovery of a pre-registered profile, if the optional GSMA Discovery Service is to be used

The M2M solution requires a more extended integration:

- EIS1 interface is used for provisioning of eSIM data to SM-SR
- ES2 interface is employed by the MNO to order profile downloads from SM-DP and to pass profile state management commands to SM-SR
- ES3 interface is an internal interface between SM-DP and SM-SR and only exposed when external RSP components are integrated
- ES4 interface is used by the MNO or an associated IoT Service Provider to manage profile states and to configure eSIM parameters on SM-SR
- ES7 interface enables the “SM-SR Change” procedure to move a provisioned eSIM device from one SM-SR to another (rarely used due to commercial complexities)

One key function for SM-DP(+) has not been specified by GSMA - the provisioning of MNO profiles - and is therefore performed utilising a

proprietary interface. Since Mobile Network Operators have established processes to manage subscriber personalisation data for

SIM manufacturing, like network authentication keys, subscription identifiers, and network parameters, the RSP solution ideally supports a two-step procedure, that can mimic existing procedures. In a first step, a pre-developed profile template is imported into the RSP system. As a second step, the profile personalisation data are imported. The RSP system can then create the profiles for eSIM download by merging the template with the personalisation data.

Beyond the integration of GSMA-specified interfaces, there is a multitude of possibilities depending on the chosen business and service model. Your RSP software provider should expose a wide range of functions with REST (Representational State Transfer), that provides a simple method of accessing its services. For the system to be future-proof, choose a software provider that is capable to deliver customisation and new features based on an agile development process that allows for quick release and deployment cycles.

Inspecting the kitchen – the GSMA security audit

Now is the time to perform the GSMA security audit that is necessary before you can request the signed certificates from the authorised Certificate Issuers (CI). This chapter provides a brief overview of the related assessment scheme, SAS-SM (Security Accreditation Scheme for Subscription Management).

SAS-SM covers the following activities within eSIM Remote Provisioning and Management:

- eSIM life cycle and processes in the scope of SM-SR
- Profile life cycle and processes in the scope of SM-DP and SM-DP+
- SM-DS processes

Each system component involves specific assets that need to be protected. These assets can be of the following types:

- Information (files, metadata, keys...)
- Processes
- Systems

All assets must be controlled and closely supervised to ensure secure storage and handling. To consider processes as being secure certain requirements must be met. These requirements are specified in the “SAS Consolidated Security Requirements” document and cover the following areas:

- Policy, strategy, and documentation, including business continuity planning
- Organisation and responsibility
- Information
- Personnel security
- Physical security
- Certificate and key management
- Sensitive process data management

- SM-DP, SM-SR, SM-DP+, and SM-DS service management
- Computer and network management

As part of the audit, the RSP Service Provider must show that the requirements are met by established processes for which evidence of correct operation exists. The GSMA audit procedure involves three phases.

Audits for SAS-SM certification are conducted on behalf of GSMA by NCC Group and SRC Security Research & Consulting GmbH.

Ready to serve – going live with the production system

When the SAS-SM dry audit has been passed successfully, preparation of the live service can begin. The production system is deployed as a clone of the staging system and its firewalls are configured in line with the expected security level. The RSP Service Provider can now generate all needed system certificates and send the Certificate Signing Requests (CSR) to the designated Certificate Issuers. This implies a significant cost for the RSP Service Provider, an area currently lacking transparency. With more companies joining the list of certified RSP providers, however, there are signs that GSMA is going to adopt its rules to safeguard an equal-level playing field between established RSP providers and those entering the market.

Once the signed certificates have been installed in the production system, approval

- Dry Audit: to obtain SAS-SM provisional certification valid for 9 months using test data
- Wet Audit: to upgrade the provisional certification to full certification using live data
- Renewal Audit: to maintain certification at the end of the full certification period

testing can be performed. It involves the following elements for the consumer RSP solution:

- Open-market, eSIM capable consumer devices
- MNO profile
- MNO subscription personalisation data
- Test cases

The M2M RSP solution additionally requires:

- eSIM capable IoT device/modem (or eSIM in a removable form factor)
- eSIM data for SM-SR provisioning
- Destination Address for SM-SR
- SMS-C (SMS Centre) link for SMS
- APN (Access Point Name) for HTTPS

With the system approval testing completed successfully, the RSP Service Provider can start to on-board MNO customers – the RSP service is ready for live operation.

Before you begin – well planned is a success half done

Successful implementation starts with a good plan (whether you build an RSP system or prepare a delicious dinner) that addresses the following core questions:

- Is the plan realistic?
- Are its objectives concrete and measurable?
- Does it include specific actions, responsibilities, timelines and budgets?

Your RSP software provider should be able to provide you with advice based on real-world experience, helping you to create a project plan that will deliver a live RSP service on time and on budget that accomplishes your defined targets. As addressed in the previous chapters, the critical element when building an RSP service is the SAS-SM audit. It must be planned and coordinated with the assigned auditors from the very beginning. The preparation of the certification, rather than a one-time effort, is a continuous task to ensure all mandated processes and documents are thoroughly applied when the audit is performed and beyond. Companies that have already undergone similar audits for certification and have advanced security and quality policies in place are certainly at an advantage over those that start from scratch. Nonetheless, with a

dedicated team and the right level of support, the GSMA SAS-SM audit is a manageable undertaking. Another vital contributor to the success of the project will be your RSP software provider and its products. Is the RSP software light-weight with an optimised application footprint? Was it designed to be easily deployable into diverse cloud environments? Is development done along the principles of Continuous Integration to minimise the risk of errors and prolonged service disruption? How much experience does your provider have to adopt the software to various infrastructure requirements? How simple, fast and secure can your software provider introduce customised features and new extensions that enable you to build competitive, highly targeted services?

In the last chapter you can read what makes **achelos** the right software provider for your RSP service. Any questions? Then let's talk – we are happy to hear from you!

Every great Kitchen has a great Team

Why achelos is the right partner for your RSP service

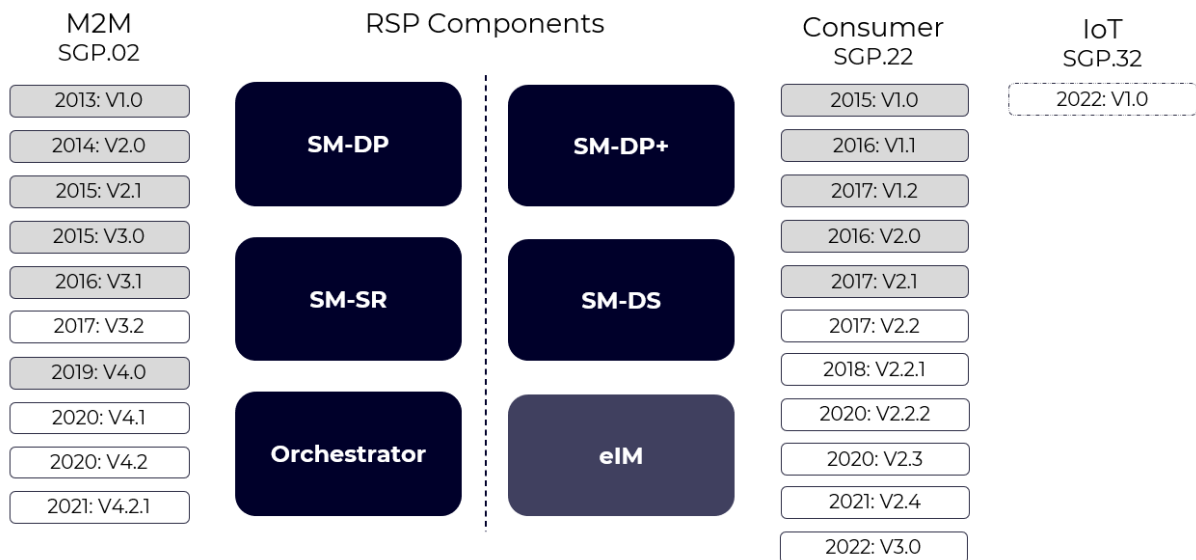
At **achelos**, we have set this target from day one: our product must be cloud-ready, no matter if public, private or hybrid cloud. Not only because we are software technology enthusiasts looking for the most up to date methods and tools, but to make sure our product is easier to use than the ones available on the market. What ease of use entails, from our point of view, is essentially ease of setup, configuration and deployment. This is why we decided to implement a microservices based architecture back in 2015, with the target to develop software completely

portable between different cloud infrastructure environments. Our software is automatically deployable in form of Docker containers in Kubernetes clusters with the help of Helm charts. Service scalability, availability and maintainability is achieved thanks to tools provided by Kubernetes. Postgres, Prometheus, ELK stack, and other state-of-the-art software. By relying on open-source technologies we have significantly reduced upfront investments as well as operational costs for the solution.

With public cloud service providers certifying their datacentre services in accordance with the GSMA SAS-SM standard in an increasing number of locations around the world, the cloud-ready architecture starts to unfold its obvious benefits:

- Rapid setup of customer PoC or trial systems, allowing our customers to get familiar with eSIM RSP Management functionality and to try it out in connection with their own business processes and backend systems
- Quick and easy setup of instances in new locations, shortening time-to-market for the introduction of new services
- Multi-site, hybrid (private/public cloud), geo-redundant and other custom configurations can be built without changing even one line of code

achelos offers a complete suite of RSP software solutions compliant with GSMA standards for consumer and M2M / IoT devices.



achelos Solution Portfolio

As an Associated Member of GSMA, **achelos** is carefully monitoring the evolution of all relevant specifications and our commitment is to constantly upgrade our solutions to offer new functionality, while ensuring compliance with the evolving specifications.

Where we are coming from

In May 2008, Kathrin Asmuth founded **achelos** as a manufacturer-independent software company to develop specialised products and services for the embedded, digital security market. Within the vertical segments Connect, Industrial IoT, eHealth, Government and Critical infrastructure, our fundamental, cross-functional competence is digital security. We help our clients to realise high-security products and services, from PKI solutions to



secure development of Common Criteria (CC) evaluated software.

In 2015, Kathrin brought together a team of experts in embedded telecom technology and cloud-ready, large scale application development, the CONNECT division. Our senior experts have been part of the mobile telecommunication industry for decades, actively contributing to the very first eSIM specifications from GSMA. Based on the vision that only a manufacturer independent RSP software would be able to truly deliver the benefits of the plastic SIM's digital transfor-

mation, the team set to work from a clean slate without any legacy code. It resulted in the world's first implementation of a GSMA eSIM RSP Management system for M2M developed by a non-SIM vendor in 2017. Since the release of the RSP consumer solution SM-DP+ in 2019 we offer a complete set of solutions to the market that grant our customers full control and ownership of the eSIM RSP management service.

What drives us beyond our enthusiasm for technology

Knowledge

The expertise of our talent pool forms the foundation of our success, and we connect the right skills with the unique requirements of each customer

Curiosity

Our curiosity is driving learning and innovation and we engage deeply with new ideas, question our assumptions and explore uncharted territory

Sincerity

Say what you mean and mean what you say - in this way we build long-lasting relationships based on transparency and fairness

Reliability

All our work is based on well-defined processes and industry quality standards to consistently produce high-quality results

Sustainability

We are committed to creating a sustainable society, actively managing our operations in a way that balances our social, environmental and economic objectives

Annex

Abbreviations

AKA	Authentication and Key Agreement
APN	Access Point Name
CI	Certificate Issuer
CSR	Certificate Signing Request
ECASD	eUICC Certificate Authority Security Domain
eIM	eSIM IoT Remote Manager
EIS	eUICC Information Set
eSIM	Popular name equivalent to term eUICC used in GSMA specifications
eUICC	Embedded Universal Integrated Circuit Card
GSMA	GSM Association
HSM	High Security Module
HTTPS	Hypertext Transfer Protocol Secure
IoT	Internet of Things
IPA	IoT Profile Assistant
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
LPA	Local Profile Assistant
LPWA	Low-Power Wide-Area
M2M	Machine to Machine
MNO	Mobile Network Operator
NAA	Network Access Application
NB-IoT	Narrowband Internet of Things
OEM	Original Equipment Manufacturer
OSS/BSS	Operations Support System and Business Support System
RSP	Remote SIM Provisioning
SAS	Security Accreditation Scheme
SAS-SM	SAS for Subscription Management
SD	Security Domain
SIM	Subscriber Identity Module
SM-DP	Subscription Manager - Data Preparation
SM-DP+	Subscription Manager - Data Preparation Plus
SM-DS	Subscription Manager - Discovery Server
SMS	Short Message Service
SMS-C	Short Message Service Centre
SM-SR	Subscription Manager - Secure Routing
TCA	Trusted Connectivity Alliance (formerly SIM Alliance)

References

GSMA SGP.01	eSIM Architecture Specification M2M
GSMA SGP.02	eSIM Technical Specification M2M
GSMA SGP.06	eUICC Security Assurance Principles
GSMA SGP.07	eUICC Security Assurance Methodology
GSMA SGP.08	Security Evaluation of Integrated eUICC
GSMA SGP.11	eSIM Test Specification
GSMA SGP.16	eSIM Compliance Specification M2M
GSMA SGP.21	eSIM Architecture Specification Consumer
GSMA SGP.22	eSIM Technical Specification Consumer
GSMA SGP.25	eUICC for Consumer Device Protection Profile
GSMA SGP.29	EID Definition and Assignment
GSMA SGP.31	eSIM IoT Architecture Specification IoT
GSMA SGP.32	eSIM Technical Specification IoT
GSMA SGP.14	PKI Certificate Policy
GSMA SGP.24	eSIM Compliance Process
GSMA FS.08	SAS Standard for Subscription Manager Roles
GSMA FS.09	SAS Methodology for Subscription Manager Roles
GSMA FS,18	SAS Consolidated Security Requirements and Guidelines
GSMA	Cloud Deployment of Subscription Management Solutions
GSMA	Budgeting for SAS-SM Certification
TCA	eUICC Profile Package: Interoperable Format Technical Specification
TCA	eUICC Profile Package: Interoperable Format Test Specification

For more information, visit:

connect.achelos.com

