achelos

Remote eSIM Provisioning

Cookbook

How to build your own
eSIM RSP Service

Table of Contents

Do-It-Yourself eSIM Provisioning

Your kitchen – your rules

eSIM is separating the non-reprogrammable SIM chip from the MNO profile and transforms the profile into a truly digital asset. Despite the obvious advantages of this approach, uptake of the technology has been slow for years, leading to limited usage where “eSIM Management-as-a-Service” from established manufacturers was the only viable option. Times are changing, however, 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. Besides the projected growth of eSIM usage, GSMA certified cloud offered by Microsoft Azure, AWS and many other cloud providers, lowers the entrance barrier for hosting RSP services significantly. It reduces efforts substantially while offering scalability combined with telco-grade reliability, enabling companies to operate an RSP service that effortlessly scales with increasing demand.

- **Solution & Service Providers** that want commercial and technical independence to offer competitive RSP services to their customers.

- **Mobile Network Operators** that want to fully control storage and processing of subscriber data in-network.

achelos offers a complete suite of RSP solutions covering the components specified by the GSM Association (GSMA) as well as solutions that go beyond the specified standards. To the challengers of the eSIM Management status quo, we deliver:

commercial **independence** | technical **autonomy** | operational **sovereignty**

With this “Cookbook” we want to 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 components required to build an RSP service that you fully control and that is enabling your business strategy in the long-term.

Flavours of eSIM

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

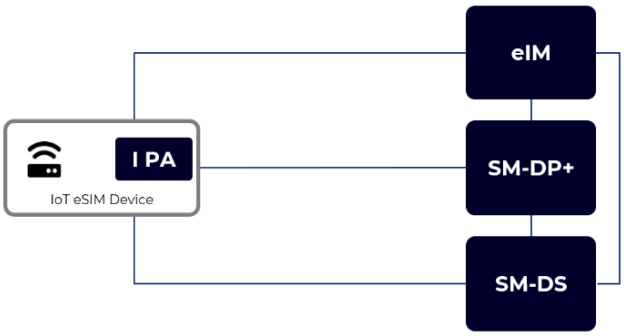
The first GSMA RSP standard released in 2010, enabling the centralised management of M2M eSIM devices, involving two system components. The SM-DP (Subscription Manager Data Preparation) securely encrypts the network access credentials (i.e., the profile) and manages the remote provisioning process. The SM-SR (Subscription Manager Secure Routing) is 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. This model requires interconnection of the systems components (DP-SR, SR-SR) via standardized interfaces, where each new connection is linked to additional efforts and costs, which has become the main roadblock for mass roll-out of this technology.

Managing eSIM for consumer devices with SM-DP+

The consumer standard (SGP.22) was published in 2015 and defines the SM-DP+ for the creation and protection of MNO profiles and an 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. In this model, the consumer device can communicate directly with the SM-DP+ of any MNO. The optionality of SM-DS and its integration with SM-DP+ dramatically lowers the barriers for the technology adoption, which has resulted in the fast growth of transactions volumes over the last years.

Utilising SM-DP+ to manage eSIM for IoT devices with eIM

The limitations of the M2M standard, especially its incompatibility with the widely used IoT technologies NB-IoT and LPWA, resulted in the latest RSP standard SGP.32. While relying on the market-proven components SM-DP+ and SM-DS, it defines a new component, the eIM (eSIM IoT remote Manager), that 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, an application is required on the device to manage the communication between eSIM and backend, the IPA (IoT Profile Assistant). This model brings together the best from the M2M and Consumer standards, combining the remote management of profile states via eIM with direct download from SM-DP+.



iSIM – same function, different form

eSIM functionality, independent of its application, can be delivered in different form factors.

Best known is the dedicated chip that is embedded into a device. In other scenarios the eSIM chip is embedded in a plastic card body like the standard SIM card and that can then be inserted into the SIM slot of a device.

With iSIM the chip is integrated into a trusted area of the main processor resulting in substantial savings of energy and physical footprint, which makes it ideal for the use in Low-Power Networks, such as NB-IoT.

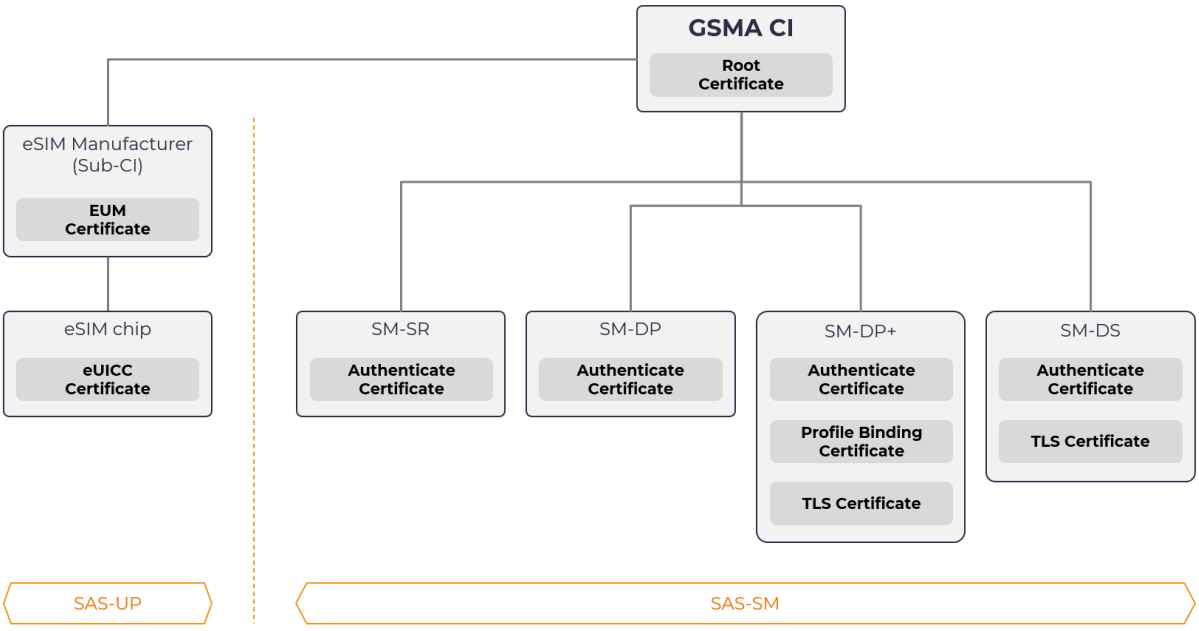
However, from the Remote Subscription Provisioning ecosystem perspective, iSIM is simply a form factor that is managed in the same way as any other eSIM form factor.

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.

GSMA Certificates – gatekeepers of the ecosystem

The GSMA has defined a PKI (Public Key Infrastructure) for the eSIM ecosystem and its CI (Certificate Issuer) issues certificates for eSIM remote provisioning system entities, acting as a trusted root for the purpose of authentication of the entities of the system. It requires each component to receive certificates signed by the PKI's CI (Certificate Issuer) or, in case of the eSIM chip, by the chip manufacturer's Sub-CI.

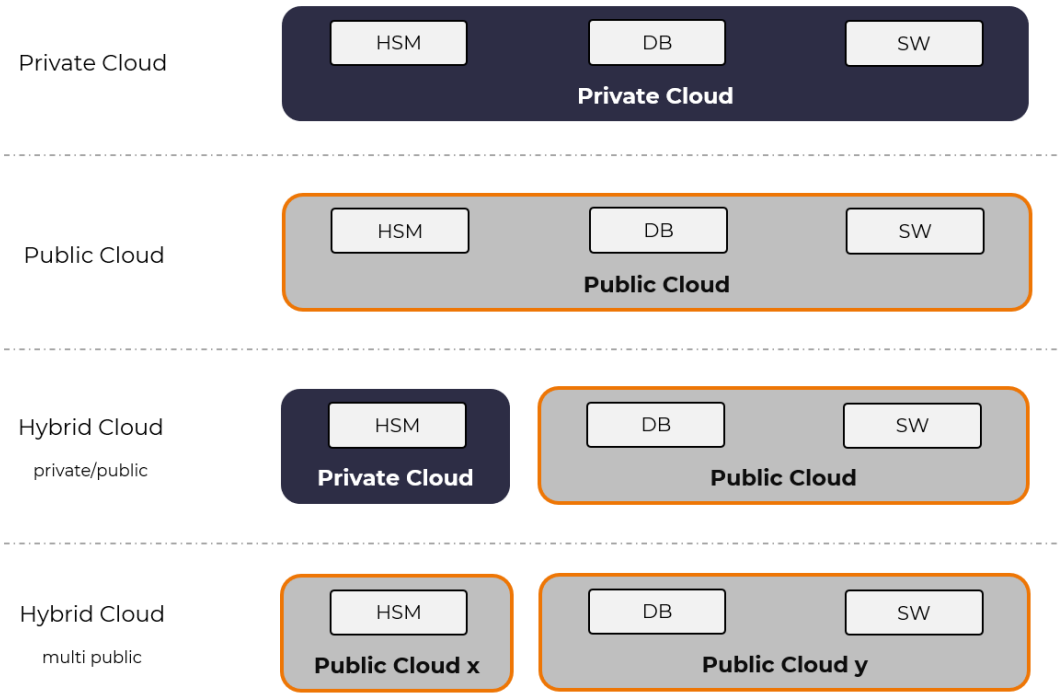


Before a company can enter the eSIM ecosystem, however, it must perform a security audit according to the GSMA's Security Accreditation Scheme (SAS). The scheme is defined in two variants, one for chip production (SAS-UP) and another one for Subscription Management (SAS-SM), which is the scheme required for operating an eSIM RSP service. Following the successful security audit, the signed system certificates can be requested, allowing the remote provisioning of profiles to any eSIM supporting device.

Infrastructure – moving to cloud

An RSP solution consists of three key components: the eSIM RSP software, the database and the Hardware Security Module (HSM). This HSM, a physical device that generates, stores, and manages cryptographic keys, is at the heart of the eSIM security architecture and can be considered as the safe home for all cryptographic applications.

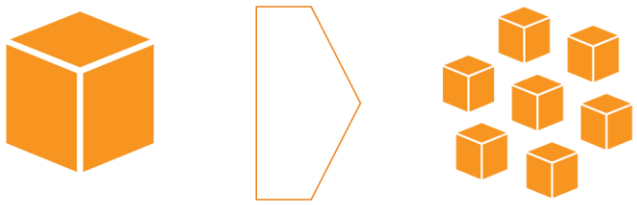
The demand for the RSP Service to be operated in a highly secure environment is adding some complexity when setting up the infrastructure. This has been recognised by a growing number of cloud service providers that have certified datacentres according to GSMA SAS-SM in regions around the globe. As a result of this multiple deployment options with respect to the key components of an RSP solution are now available, as shown below:



Especially when selecting the HSM, it is necessary to consider GSMA's Security Accreditation Scheme. The compliance requirements for Hardware Security Modules and their hosting environments focus on security assurance, functionality, and interoperability, specifically, the "[...] storage and cryptographic computation for keys and certificate generation [...] shall rely on hardware security modules (HSM) that are FIPS 140-2 level 3 certified."

RSP Software – cloud-native from day one

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. To avoid these pitfalls, our achelos eSIM RSP solutions are designed based on a microservices architecture and packaged in containers.



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 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 from them. 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

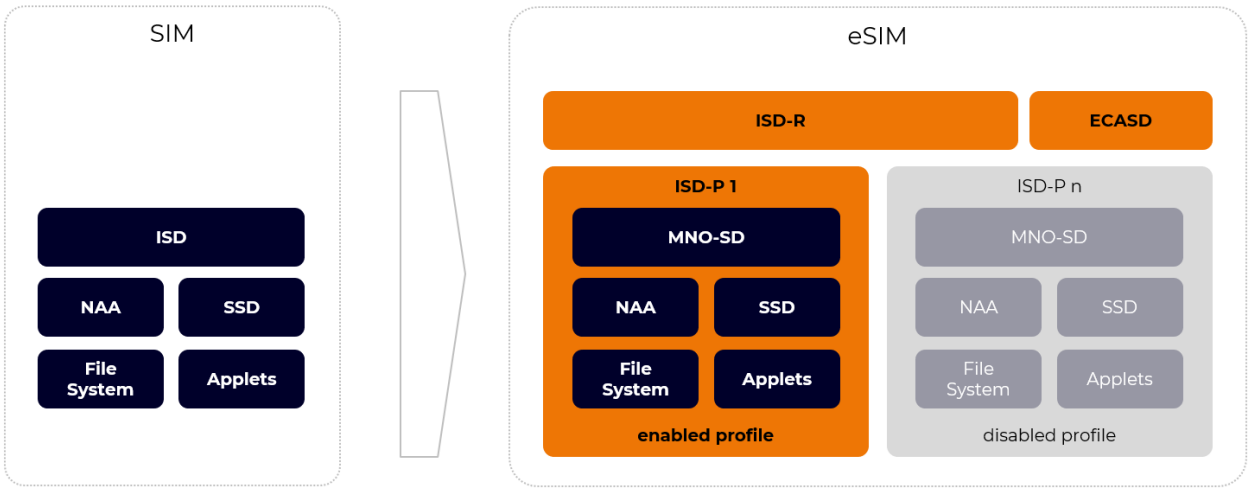
MNO Profile – virtualisation of the SIM

The core functionality of the operator profile, from inception of the first digital mobile standard GSM to the latest releases, is the storage of subscriber credentials and the implementation of algorithms and applications used for mutual authentication of subscriber and network.

The profile's 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 highly secure capabilities to remotely load and manage multiple profiles.

To accomplish this 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



The eSIM MNO profile, however, is essentially identical with a SIM profile and 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 work across different platforms, the industry agreed to use a standardised description of its content and therefore MNO profiles for eSIM shall comply with the format defined in the “Interoperable Profile Package Description” specification of the Trusted Connectivity Alliance (TCA).

The specification is intended primarily for eSIM Service providers, Profile Creator users, for example Mobile Network Operators and eSIM hardware vendors enabling them to elaborate and exchange profiles with guaranteed interoperability.

```
peHeader ProfileElement ::= header : {
  major-version 2,
  minor-version 0,
  profileType "achelos TestConsumerProfile",
  iccid '89491000000000000001'H,
  pol '00'H,
  eUICC-Mandatory-services {
    usim NULL,
    milenage NULL,
    javacard NULL
  },
  eUICC-Mandatory-GFSTEList {
      {2 23 143 1 2 1},
      {2 23 143 1 2 4},
      {2 23 143 1 2 5},
      {2 23 143 1 2 7},
  },
},
mfVal ProfileElement ::= mf : {
  mf-header {
    mandated NULL,
    identification 1
  },
  templateID { 2 23 143 1 2 1 },
  mf {
    fileDescriptor : {
      pinStatusTemplateDO '01020A0B'H,
    },
  },
  ef-pl {
    fillFileContent : 'FFFF'H,
  },
…
```

Master Recipe

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

Turn on the heat – putting the infrastructure in place

The three key components of the eSIM RSP solution, the eSIM RSP software, the database and the Hardware Security Module, must be logically as well as physically protected and therefore choosing the right location for the physical infrastructure is the very first step. It can be on-prem, at a third-party co-location data centre or with a public cloud service provider.

Many telco organisations are moving towards public cloud for various reasons: scalability, reliability, service continuity and more. However, there are use cases where a private cloud can be the preferred solution. Maybe to utilise existing infrastructure or because the RSP service is intended for less critical applications as can be the case with Mobile Private Networks, one of the upcoming markets for eSIM management. Our software solutions support any scenario since it can be deployed in any containerised environment.

Special consideration should be given to the HSM because it can't be a virtual asset shared across several tenants but must be a dedicated machine. This is in strong contrast to the principal function of Public Cloud Service Providers that find it difficult to offer attractive solutions.

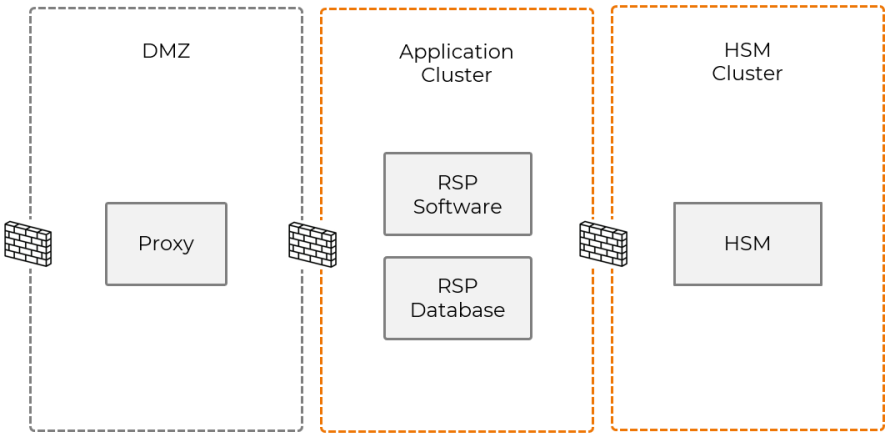
Our partner Utimaco, one of the world's leading HSM manufacturers, makes this complex part of the eSIM service much easier to navigate with a true HSM-as-a-Service offer. It includes dedicated HSM hardware, hosted at UTIMACO's certified data centres with 24/7 access to expert support. This service can remarkably simplify hosting of an eSIM service and reduce capital expenditure considerably.

You can read more information in chapter HSM Solutions by *Utimaco*.

Stir until combined – deploying the RSP solution

Once the infrastructure is in place, the eSIM RSP solution can be deployed. Following best practices we recommend building a pre-production staging environment as well as a production system.
The staging system is crucial for the lifetime of the RSP service and plays a key role during release testing, upgrades and incident resolution but also for the initial SAS security audit required to receive the signed certificates for the production system.

The high-level architecture will always be quite similar, consisting of a secure network for the application and a DMZ (De-Militarised Zone). The DMZ is deployed between firewalls that screen all inbound traffic and is restricting remote access to the eSIM service resources located in the secure network. Depending on your risk profile you can even have a third firewall to specifically protect access to the HSM.



The actual implementation is always distinct for each deployment, depending on your chosen service configuration, service level expectation and preferences regarding infrastructure location and software utility components.

achelos is in a unique position to support the solution planning and deployment process with in-depth knowledge from years of experience as well as an expert network of world-leading partner companies. In close cooperation with you we ensure that your eSIM service is built in the most effective way, that meets - by design - your requirements as well the ones of the SAS security scheme.

You can read more information in chapter eSIM RSP Solutions by *achelos*.

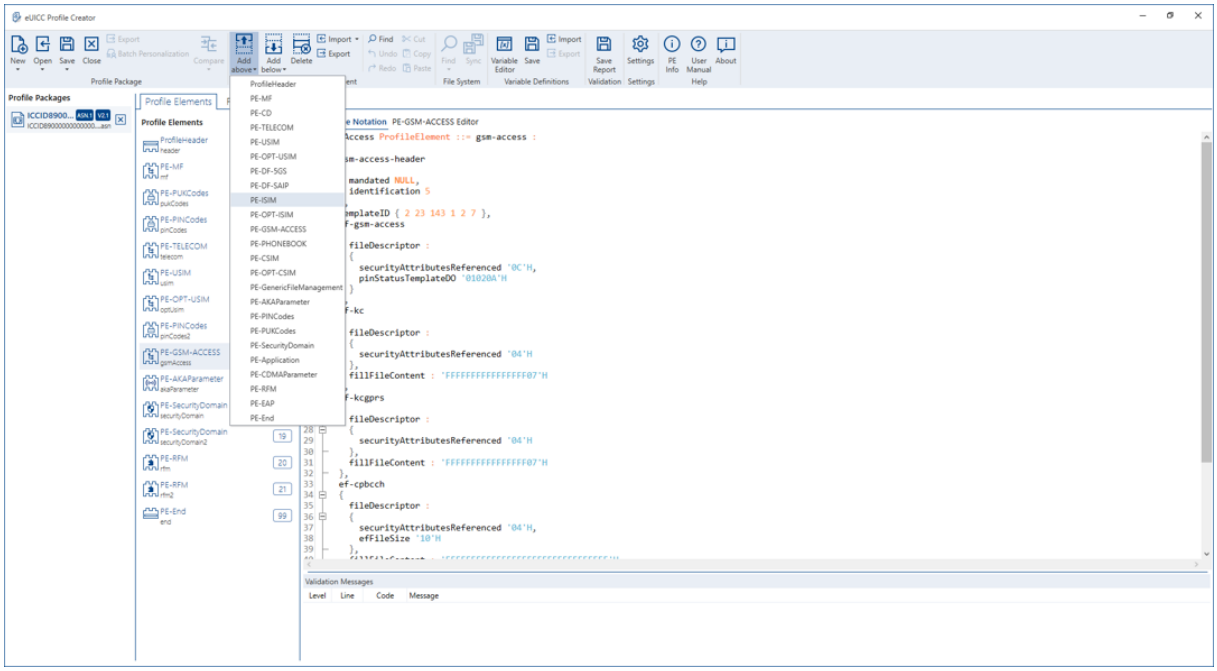
Season to taste – creating the eSIM profile

Because the profile was an indivisible element of the plastic SIM it usually was developed by the SIM manufacturer 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 comes at a price - there are now few applications that 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, even though smartphones manage this function anyway.

eSIM continues to change the landscape and more specialised companies with expert domain knowledge now offer MNO profile development, either as a service or through open-market tools. It is not only much more efficient but also provides complete ownership of the profile.

Our partner COMPRION, a leading, globally recognised provider of eSIM test solutions and services, offers the “eUICC Profile Creator”, a tool for the GUI assisted development of profiles with automated validation against the relevant industry specifications (3GPP, ETSI, GlobalPlatform, GSMA, TCA).



Furthermore, COMPRION operates the TCA eSIM Interoperability Test Service. You can read more information about this in chapter Profile Development & Test Tools by *COMPRION*.

Inspecting the kitchen – the GSMA security audit

The next step after the eSIM RSP solution has been deployed and fully configured is the security audit. As part of the audit, the RSP Service Provider is expected to show that the SAS defined requirements are met by established processes for which evidence of correct operation exists.

The requirements are specified in the "SAS Consolidated Security Requirements" document from GSMA and cover multiple areas across the organisation (with focus on the eSIM Service) like:

- Organisation, responsibilities, policy, strategy, documentation and information
- Personnel security
- Physical security
- Sensitive process data management
- Certificate & keys management
- Computer & network management
- RSP service management

Because of these wide-ranging requirements, we recommend starting the preparation of the security audit as early as possible. achelos, together with our partner SRC (Security Research & Consulting), one of the two GSMA accredited auditors, can help to ensure that your SAS certification is achieved in the most efficient way.

We explain in detail how the process works and discuss with you the optimal service setup for your particular deployment. We can help you to identify any gaps within the security organisation and provide precise guidance how you get to the expected level of compliance. Your preparations can then be validated with a pre-audit before the official dry audit for provisional certification takes place.

Following the successful dry audit you can purchase the certificates from the designated Certificate Issuers and launch your RSP Service. Within nine months the wet audit is required for full certification.

You can read more information in chapter GSMA SAS Consulting by *SRC*.

Every great Kitchen has a great Team

A partner ecosystem for end-to-end success of your eSIM RSP Service.

In the dynamic realm of technology, partnerships are the cornerstone of success. Collaborating with complementary technology partners allows to combine expertise, resources, and technologies, resulting in more robust and competitive offerings.

We strongly believe that the value of cooperating together cannot be overstated in today's interconnected telecom technology landscape. By leveraging each other's strengths, specialized skills and unique expertise, we create solutions that deliver greater value to our customers.

eSIM RSP Solutions by *achelos*

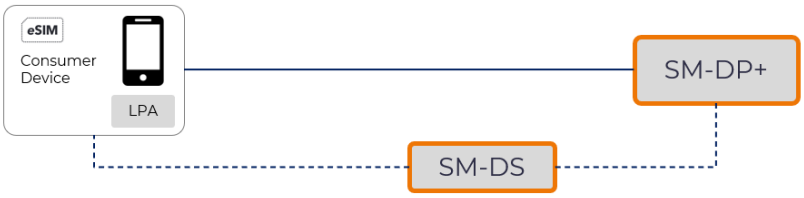
achelos is the right partner to take your idea from concept to reality!

Based in Paderborn, Germany, we are a team of embedded cryptography and telecom experts enabling high-security services for the management of mobile network identities. Looking beyond one-fits-all solutions we provide a differentiated approach to deliver high-value results. We work with you from initial idea to ongoing support, providing you with the attention and commitment you deserve.

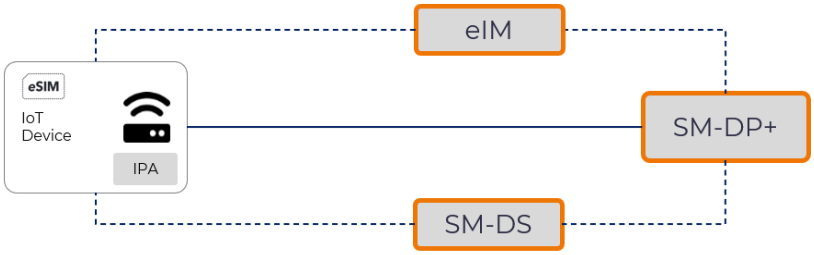
That is how we become a trusted technology partner deeply invested in your long-term success.

We offer a complete suite of RSP software solutions compliant with GSMA standards for consumer, M2M and IoT devices. With the achelos Consumer solution, Telco Solution Providers can extend their existing portfolio with eSIM Management capabilities, while Mobile Operators, especially on a group level, can harmonise the eSIM provisioning service in-network with complete control over data storage and processing.

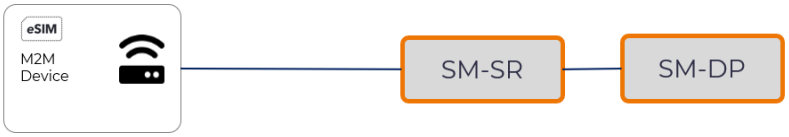
We have designed our SM-DP+ with integrated SM-DS component to be efficiently deployed into your preferred environment. Beside the standard ES2+ interface the extensive REST API of our solution allows easy integration with external systems and processes.



The cost-sensitive nature of IoT makes eSIM management a valuable asset for MNOs, MVNOs, Service & Solution Providers as well as Chipset and Device manufacturers. With SGP.32 a modern standard is becoming available based on SM-DP+ and SM-DS, introducing eIM (eSIM Remote IoT Manager) to support constraint devices in a flexible way.



For legacy management of devices compliant with the initial eSIM M2M standard we offer an integrated, efficient solution with SM-SR and SM-DP components.



For the upcoming market of Mobile Private Networks and the organisations, private as well as public, that increasingly deploy them, achelos offers an 'eSIM RSP-in-a-box' solution with minimum footprint, that guarantees the isolation of critical network keys and device identities in security sensitive environments.

Our solutions have been developed from day one to be cloud-ready, no matter if public, private or hybrid cloud. With public cloud service providers certifying their datacentre services in accordance with the GSMA SAS standard, the cloud-ready architecture starts to unfold its obvious benefits:

- Rapid setup of 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 and fully custom configurations can be built without changing even one line of code

utimaco®

HSM Solutions by *Utimaco*

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

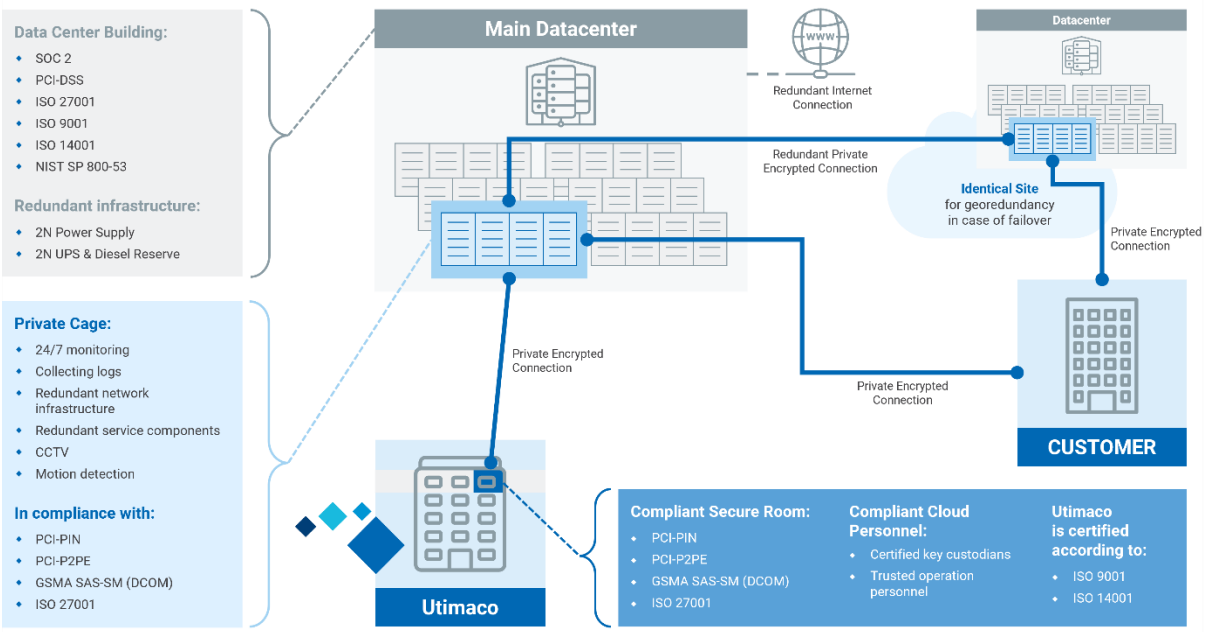
UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. UTIMACO is one of the world's leading manufacturers in its key market segments.

The Utimaco CryptoServer Cloud is the Hardware Security Module as a Service that integrates seamlessly with Cloud Service Providers. It offers the same level of security as with an on-premise HSM without having to worry about setting up the infrastructure.

CryptoServer Cloud - The HSM as a Service by Utimaco

- No set-up and hardware efforts – but full remote control
- FIPS 140-2 Level 3 Validation
- Hosted in a ISO/IEC 27001, HIPAA, and PCI compliant data center
- Key management and GSMA SAS-SM certification support

utimaco®



The Hardware Security Module for your multi-cloud environments

CryptoServer Cloud offers the flexibility, security and reliability to enable remote eSIM provisioning in Cloud environments:

- FIPS 140-2 Level 3 HSM hosted by Utimaco
- Reduces your CAPEX – no acquisition costs, high expenses for a secure server room, and effort for hardware
- Seamless integration with all major Cloud Service Providers
- Supports multi-cloud deployments
- Fully protects your cryptographic keys and custom code
- Designed with crypto agility in mind, and is field-upgradeable with PQC algorithms recommended by NIST and BSI
- Easy development and testing with a free simulator
- Support directly from the HSM vendor: 24/7 support included

COMPRION

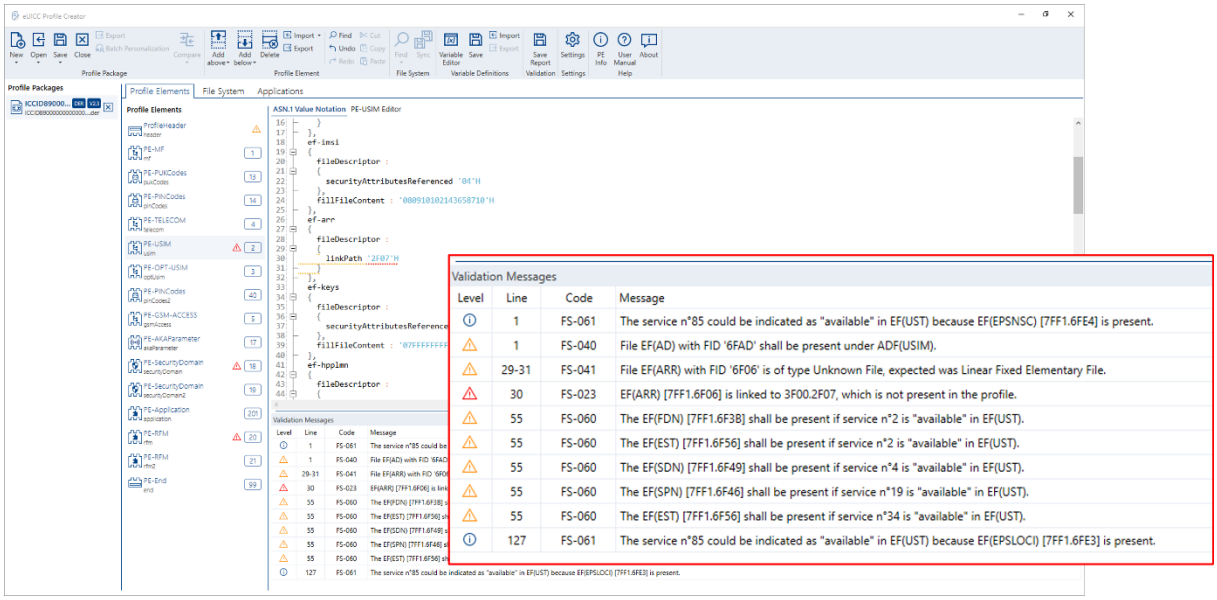
Profile Development & Test Tools by *COMPRION*

COMPRION is a privately owned, German company that provides tools, test solutions and services for the interfaces of the connected world.

With our tools, customers worldwide test smartphones, eSIMs, IoT modules and NFC devices according to the latest industry standards and beyond. In this way, COMPRION helps companies in the telecommunication, automotive and payment markets to prevent problems in the field and expensive recalls. COMPRION´s test solutions ensure, that customers can equip their products and services with the highest possible quality and interoperability.

eUICC Profile Creator

The eUICC Profile Creator is a tool to improve speed and quality of SIM profile development according to the profile package standards of the Trusted Connectivity Alliance (TCA).



You can create / edit / modify a profile. But it is much more than a normal text editor would do, e.g.:

- If you create a profile, you do not need to start from a blank sheet. The tools facilitate you to start with default templates for the various profile elements accoding to the specifications.

- Changing any configuration in the profile does not require to do any manual HEX encoding. You can rely on translators, which convert the HEX-based config into human-readable content, which you can easily edit.

- The tool contains a rules engine, which checks the profile against the relevant technical standards from ETSI, 3GPP and TCA - preventing bugs.

- Comparing two profiles does not compare the text-notation of the profile. Profiles with the same configurations can be coded in different ways. Instead, the actual configurations are compared.

TCA eSIM Interoperability Service – delivered by COMPRION

With eSIM awareness and adoption continuing to build, interoperability is key to promoting consumer trust and realising the full, transformative potential of the technology. The TCA eSIM Interoperability Service – delivered by COMPRION – enables operators to test how their eSIM profiles interact with an extensive range of consumer eSIM devices, such as smartphones, wearables, tablets and laptops, to identify and address individual interoperability and compatibility issues prior to deployment.

This is particularly beneficial for organisations with limited resource to perform comprehensive in-house interoperability testing.

SRC

GSMA SAS Consulting by *SRC*

SRC (Security Research & Consulting GmbH) was founded in 2000 and is a consulting lead for IT security. SRC bundles highly up-to-date know-how in the fields of IT security and information technology. Supported by the banking industry, SRC Security Research & Consulting GmbH represents a central link between research and products or services.

SRC has been involved in the audits of SAS-SM since the framework was first piloted in 2016, and since that time, have not only conducted audits but also helped in the development of the standards and audit methodology. This has included enabling the auditing of cloud service providers, initially as they supported certification of other companies and then as certified companies in their own right.

SRC is also recognised as a consultancy service provider for GSMS SAS-SM. We have developed a standard set of consultancy packages in order to support companies gaining certification of SAS-SM.

In addition, we also offer complementary consultancy, which is intended to be tailored to meeting the needs of a company's project and fill any gaps.

The SRC mission.

We use our know-how to support our customers in the development and implementation of secure systems. Innovation and sustainability are essential characteristics of our services. Together with our customers we create standards for secure systems and enable our customers to do better business "with security".

The SRC values.

A values-based culture is the common denominator of our work. SRC is committed to ensuring long-term security of our customers' IT security. At the same time, SRC is a company that attracts, excites and develops outstanding personalities and provides them a professional home.

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	Hardware 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

External Resources

https://connect.achelos.com/en/

https://utimaco.com/

https://www.comprion.com/

https://src-gmbh.de/en/

https://www.gsma.com/esim/

https://www.gsma.com/security/security-accreditation-scheme/

https://trustedconnectivityalliance.org/technology_overview/esim/

achelos

For more information, visit:

connect.achelos.com