Rise of the eSIM

Version: 2022-09

Table of Contents

Introduction

Since its introduction, the SIM card has become one of the world's most widely recognized security tokens, allowing mobile subscribers to securely authenticate onto the network of their wireless service provider. As with many electronic media that have come and gone in the last 30 years, the SIM is on a path to obsolescence and it will be fully replaced by a digital SIM, called an eSIM. This whitepaper provides a brief overview of the evolution of the SIM card, the processes underlying its production and introduces the reader to eSIM technology, its benefits and how wireless service providers and enterprise network operators can transform their business operations through RiPSIM's Software Suite.

A Brief History of the SIM Card

The subscriber identity module, also known as the SIM card, was conceptualized in 1989 and the first commercial SIM was deployed in Finland in 1991. Since that time, the SIM has experienced an incremental evolution primarily centered around four pillars: 1.) architecture, 2.) operating system, 3.) physical form factors and 4.) processing speed, much in the same way other electronic devices have evolved, however, in the SIM industry, the evolution did not keep pace with other technological advancements during that same period. The result led to products that were only nominally better in performance while the physical form factors got smaller by cutting away more plastic from the plug-in chip and later reducing the number of contacts on the chip from 8 pins to 6 pins (See image below).

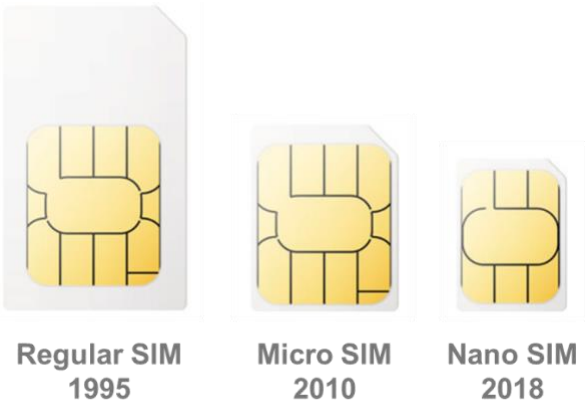

FIGURE 1- EVOLUTION OF THE PLUG-IN SIM

While the plug-in SIM form factor was shrinking, and as the wireless industry began entering Internet of Things (IoT) markets, a new kind of SIM form factor was introduced allowing it to be soldered into a device, making it more robust for applications that had greater vibration, a wider range of temperature and humidity tolerances and required data retention capabilities up to 17 years. This new form factor was called the MFF2, or machine-to-machine form factor, and today this chip is frequently found in

automobiles, power meters, remote video cameras and other applications where environmental conditions are harsher.

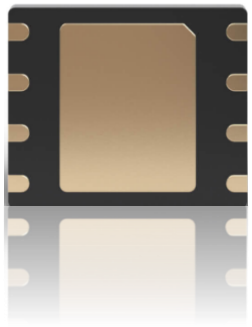

FIGURE 2 - MACHINE-TO-MACHINE FORM FACTOR (MFF2)

The introduction of the MFF2 pushed SIM vendors to upgrade manufacturing facilities as they required new production processes and equipment. In recent years several additional form factors have been introduced, the smallest of which called a WLCSP (Wafter Level Chip Scale Packaging) has been adopted for use in devices such as smart watches, where printed circuit board real estate is very limited. At approximately 1mm x 2mm in size, about the size of George Washington's nose on the face of the U.S. quarter dollar coin, the footprint of the WLCSP is exceptionally small, about 1/3rd of the size of an MFF2, and it was the last physical form factor before the SIM functionality is integrated into the System-on-Chip (Soc).

In 2010 a new IoT use case emerged that enabled a wireless service provider, or its enterprise customer, to remotely change the subscription from one wireless carrier to another. This new use case was called Subscription Management (SM) and utilized an eSIM, or electronic SIM, which could be downloaded over the air. Using this technology, enterprise customers could enter into a services agreement with one wireless carrier, and if at any time in the future, the customer demanded better network quality, more advantageous pricing, or local network coverage in a foreign country, it enabled the customer to switch carriers, without the need to physically replace the SIM card.

By 2016 eSIM technology started gaining acceptance at wireless service providers and many consumer device manufacturers began adopting the technology. Because of its small footprint on the printed circuit board, the embedded SIM gained popularity for implementation in compact devices such as tablets and wearables. Apple initially introduced the Apple SIM, an eSIM-enabled SIM card inserted into a cellular-enabled iPad, giving consumers the option to select a data plan from one of many available wireless service providers. Later, when the connected Apple Watch was launched, it too used the embedded form factor as it allowed Apple to produce a product that was both thin and sleek. In 2017, Apple was the first major handset manufacturer to integrate eSIM technology into its iPhone product line, giving consumers the option of using a digital or a physical SIM. The technology has been implemented in all Apple iPhone models since then, and on September 7, 2022, Apple announced that the iPhone 14 would ship without a SIM card tray for the North American market, marking the tipping

point for eSIM technology to be embraced universally. Other notable handset manufacturers, such as Samsung, Motorola, and Google have implemented eSIM technology in recent years and will likely follow Apple's lead and eliminate the pluggable SIM.

What is an eSIM?

With all of the talk about the SIM card entering its sunset and the eSIM poised to be its successor, one might ask what is an eSIM? An eSIM is a fully digitized edition of the SIM card and like the SIM card, it is used to securely authenticate mobile subscribers onto the networks of the issuing wireless service provider. It is comprised of a series of files, file structures, and secret keys called a Profile template which has been built by interpreting thousands of pages of industry technical specifications. Profile templates may contain upwards of 200 files with each one needing to be properly configured. Below is a simplified illustration of a single eSIM file structure.

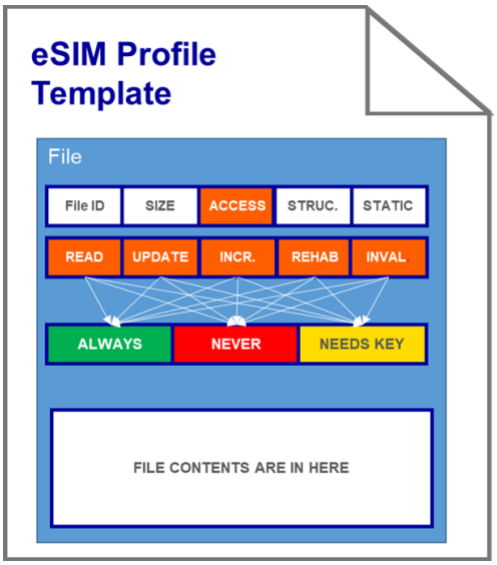

FIGURE 3 - SIMPLE SIM FILE ILLUSTRATION

Today, the design of the eSIM profile template is performed by traditional SIM vendors and, when completed, it is married with the unique subscriber data to create unique eSIMs. Once developed, the eSIMs are loaded into an eSIM "router" which is used to securely download the eSIMs to an awaiting eSIM-enabled device, such as a smartphone, wearable or a connected IoT device.

Rather than sourcing and installing a physical SIM card, the eSIM is installed on an awaiting consumer device remotely, using Internet connectivity and a "pull" mechanism. This can be done through one of three ways: 1.) it can be seamlessly installed using a "My Carrier" application that has been downloaded from the Apple or Android marketplaces, 2.) it can be installed by scanning a QR code that is presented on a web browser or 3.) it can be transparently installed, without the need for user intervention, by using a "Discovery Service" that is bound to the wireless service provider's billing system. For machine-to-machine use cases, the eSIM package is identical, but it is delivered to an

awaiting device by way of a “push” mechanism where a wake-up message is sent to a receiving device and opens a channel for the eSIM to then be delivered. This latter use case is generally adopted by enterprises that have large numbers of connected devices such as automobiles, trucking fleets, power meters, alarm systems and so forth.

The eSIM – a new paradigm but still the same old processes

The introduction of eSIM technology did not result in its rapid adoption. In its early years, wireless carriers had strong reservations about its utility. While the functionality of the eSIM is the same as a traditional SIM, carriers were reluctant to embrace this technology citing the ease with which its customers could switch to a competitor. While commercial relationships were governed by binding agreements, concerns remained about the adoption of this new technology and the investments needed in back-office systems to support it. Among one of the greatest barriers to mass adoption were the SIM vendors themselves.

To successfully pivot from a manufacturing paradigm into a digital one requires vision, investment and an appetite for risk that is commensurate with the desire to disrupt an industry. Rather than seizing the opportunity to take charge and aggressively invest in eSIM technology, the leading SIM vendors approached the nascent market opportunity with tepid enthusiasm. Unlike Amazon, Netflix, Spotify, and so many other digital success stories, the SIM industry was overly conservative in embracing the new paradigm and seemed content for iterative success. Nowhere was this more evident than in their backend processes.

At a time when digitization of the SIM card introduced the opportunity to digitize the entire eSIM development processes, SIM vendors elected to make only iterative changes to its backend processes to support the eSIM. Its customers were forced to follow the same inefficient procurement processes as a physical SIM… purchase order by purchase order, eSIM by eSIM, download by download. Sadly, as the technology became more prevalent, customers of SIM vendors had to wait weeks for eSIMs to be generated and delivered rather than receiving them in real-time.

To demonstrate the inefficiencies of the existing business models, the illustration below represents a hypothetical eSIM lifecycle flow between a wireless service provider in the United States and a globally leading SIM supplier. Using SAS (Security Accreditation Scheme) data obtained from the GSMA website, we have outlined the steps of a hypothetical relationship between a wireless service provider and a global SIM supplier.

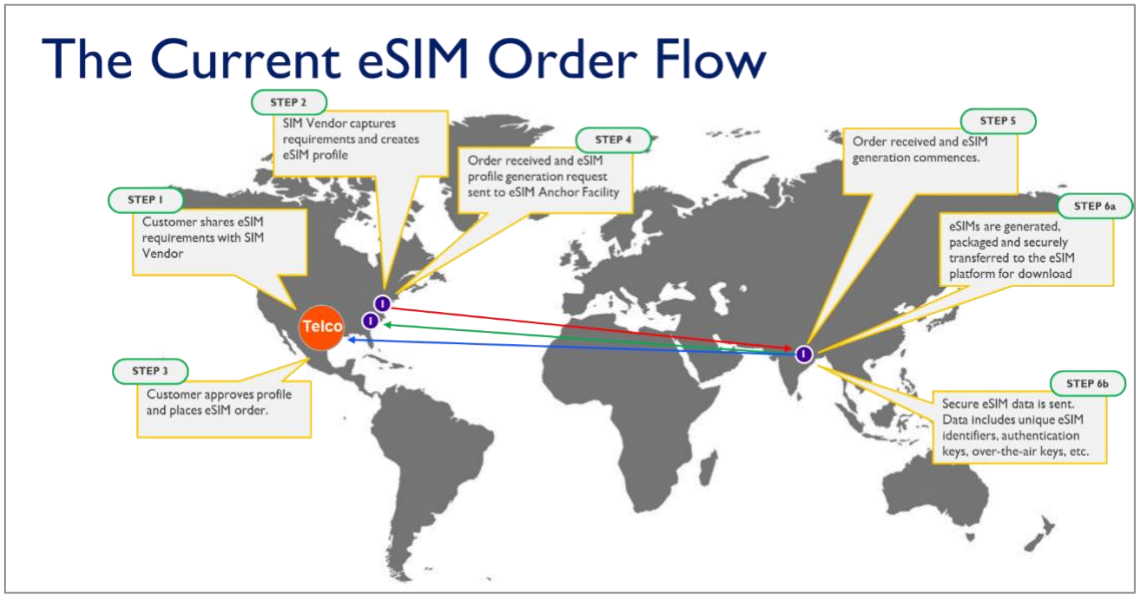

FIGURE 4 - ESIM ORDER FLOW

The figure above details the main steps involved in the eSIM design and development process before an eSIM can be downloaded to an awaiting eSIM-enabled device.

Step 1: Before an eSIM can be created, a wireless service provider shares its technical requirements with its SIM vendors. During this phase, certain secret keys are exchanged, secure data transfer requirements are established, and the eSIM technical template, called a Profile, is defined.

Step 2: Upon receiving the requirements, the eSIM vendor assigns a technical consultant to create a profile. The profile is comprised of a series of files and file structures that make it unique to each customer. During this phase, authentication algorithms are finalized as are a series of other carrier requirements such as roaming lists, over-the-air configurations, java applets and other network related criteria. Once the profile template has been completed, it is prepared for eSIM production. While it may seem this process is fast, the fact is that in many cases a brand-new profile templates can take up to 20 weeks to complete, while an iterative profile template update can take 2 to 4 weeks.

Step 3: Once the wireless service provider and the eSIM vendor agree that the profile has been properly created and tested, the wireless service provider places a purchase order for a desired quantity of eSIMs and supplies a corresponding "input file" containing instructions on which data ranges to use in the eSIM production process. For many SIM vendors receiving purchase orders and placing internal job requests is not an automated process and it may take three to five business days for a wireless service provider to receive an order acknowledgement.

Step 4: At this stage, with the purchase order and corresponding input files received, the eSIMs could be immediately generated, but this is not the case. Many eSIM vendors have established globally distributed eSIM foundries where the eSIMs are generated, packaged, and encrypted and until an internal order is placed between the eSIM vendor field office and its eSIM foundry all activities are idle. In the illustration above, the foundry is in Noida, India.

Step 5: Upon receiving the internal instructions from the SIM vendor's field office, the eSIM foundry places the order into its production queue, but since the foundry is responsible for servicing a multitude of global customers it can take up to several weeks for the eSIMs and the

corresponding eSIM data to be delivered. In essence, wireless service providers must wait their turn in line.

Step 6a – Once eSIM production capacity has been slotted, the eSIM foundry starts generating the eSIMs. Here profile templates are "married" with securely generated secret keys to create the eSIMs, each containing a unique identity. Depending on the quantity and system resource availability, this process can be completed in a matter of minutes for small batches and up to 24 hours for large production runs. When the job is complete, the eSIMs are transferred and loaded into an awaiting eSIM "router" (called an SM-DP+ for consumer devices and SM-DP/SM-SR for M2M devices). Depending on the eSIM infrastructure, this process may be seamless, or it may have an intermediary step where the eSIMs must first be downloaded to a secure intermediary location and then later installed in the "router" by a staff member.

Step 6b – While the newly minted eSIMs are being loaded into the eSIM "router", the operational eSIM data is securely transferred to the wireless service provider. This is most commonly done by posting the data to a Secure File Transfer Protocol (SFTP) server or sent via encrypted email to a designated employee. Upon receipt of the data, the wireless service provider loads the data into its respective network elements e.g., authentication center, SIM OTA and billing system, and from thereon eSIMs can be downloaded and activated as needed.

When considering the many steps detailed above, one can easily conclude that there is tremendous opportunity for workflow and security improvements. Not only are there many human interactions across the eSIM journey, but the mere fact that the data is geographically fluid, means that at each step in the eSIM generation journey there are opportunities for mistakes to made and for data to be corrupted or compromised or intercepted. While the SIM vendors have well established security practices, the probability of something going amiss increases with each step. The irony is that virtually all the laborious steps can be streamlined using modern technology in ubiquitous cloud environments, allowing for faster profile template creation, near-real-time eSIM generation and a seamless transfer of eSIM data to the awaiting "router." At RiPSIM Technologies we have done just that!

RiPSIM – The New eSIM Paradigm

With the introduction of 5G, mobile network operators have begun accelerating the migration of their wireless architectures to the cloud. As the technology becomes increasingly more software-defined, it presents unparalleled opportunities to not only lower operational costs, but also to create newer and more efficient workflows. RiPSiM Technologies is at the cutting edge of the eSIM lifecycle transformation by enabling wireless service providers to reclaim full control of their eSIMs. Using the RiPSIM Software Suite, wireless service providers can now be liberated from their dependencies on SIM vendors and design their own profiles, develop their own eSIMs and download them via their own eSIM router all from a secure cloud environment.

RiPSIM Software Suite

Keeping identity and personal information on mobile devices secure is paramount to consumers and enterprises alike. RiPSIM empowers customers such as wireless service providers and 4G/5G private

networks to design, develop and deliver digital identities (aka eSIMs) any time, for any device, in any quantity and with the highest security level in the industry.

The RiPSIM Software Suite is a fully integrated eSIM ecosystem comprised of three modules which efficiently enables eSIM lifecycle management: 1.) the design studio, 2.) the eSIM development engine, and 3.) the over-the-air eSIM delivery router.

FIGURE 5- RIPSIM SOFTWARE MODULES

eSIM Design Studio

The first proprietary module is the design studio which features an intuitive web-based user interface allowing a user to create a profile template using either Wizard or Expert mode. Wizard mode, known as eWIZ®, guides the user, whether an eSIM novice or an expert, step-by-step, through a series of questions culminating in the successful creation of the profile template, a technical specification comprised of files and files structures that are the embodiment of the eSIM. Expert mode, the interface for the more seasoned user, introduces a novel drag-and-drop interface, as well as detailed views that allow the user to define template elements at the most granular level. Both modes have been designed with inline quality controls, meaning that any structural mistakes or omissions that are made in the profile template are immediately flagged by the software for correction. For example, if the user enters an incorrect length in a number field, the software will specify the length needed based on the requisite TCA, GSMA or 3GPP specification. Once the user has successfully completed the steps, the output of the design studio is a 4G, 4G/5G, or 5G profile template that the user needs to proceed to the second step, generating a unique eSIM for a device.

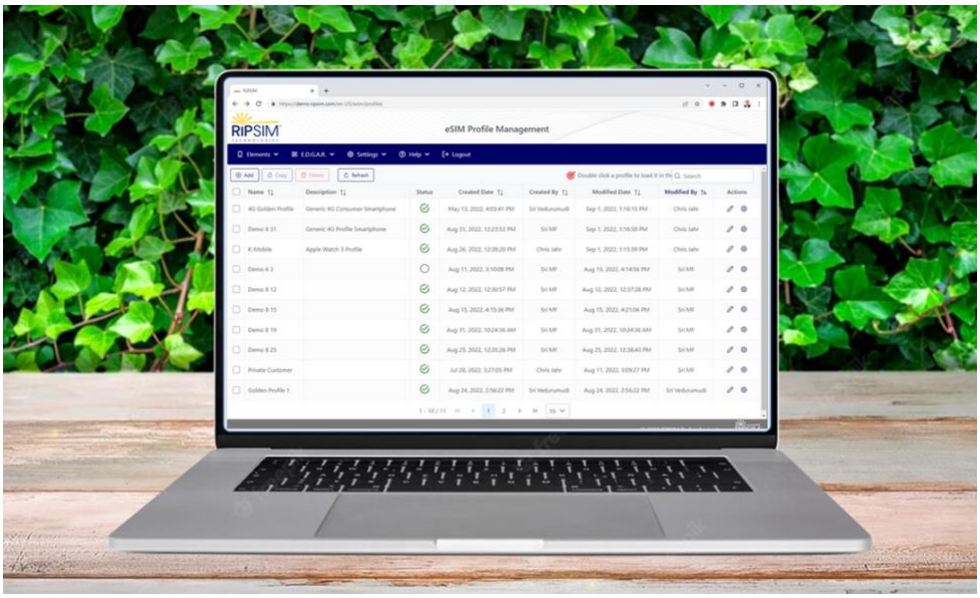

FIGURE 6 - RIPSIM EWIZ

eSIM Development Engine

The second proprietary module is RiPSIM's eSIM development engine. It lies at the heart of the RiPSIM ecosystem and is the engine that generates and encrypts individual eSIMs on-demand, allowing users to create as few or as many as they need – from one to millions. The ability to scale to the user's needs comes from RiPSIM's highly elastic microservices-based design which employs the most contemporary services architecture, using system resources only when needed. eSIM generation is done in real-time, using RiPSIM's incremental generation methodology; it is based on a profile template created in the design studio married with the unique subscriber parameters for each device in the field.

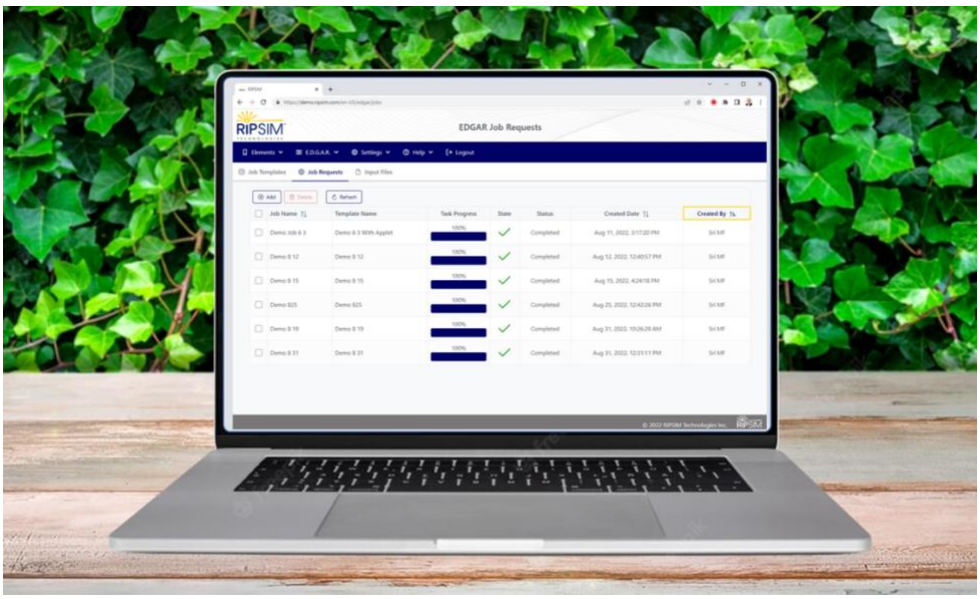

FIGURE 7 - RIPSIM ESIM ENGINE INTERFACE

eSIM Secure Router

The third module is used to securely store and download the uniquely generated eSIMs "Over-the-Air" (OTA) when pinged by an awaiting mobile device. The delivery module is commonly referred to in the wireless industry as an SM-DP+ (Subscription Management – Data Preparation). Through the use of industry standardized application programming interfaces, eSIMs can be downloaded to awaiting devices in one of several ways, including: through the scanning of a QR code via a web portal, as shown in the image below, or by integrating a download feature in a wireless service provider's iOS and Android applications, or via a discovery service[1] where the mobile device "asks" a third-party service to determine if an eSIM is waiting to be downloaded.

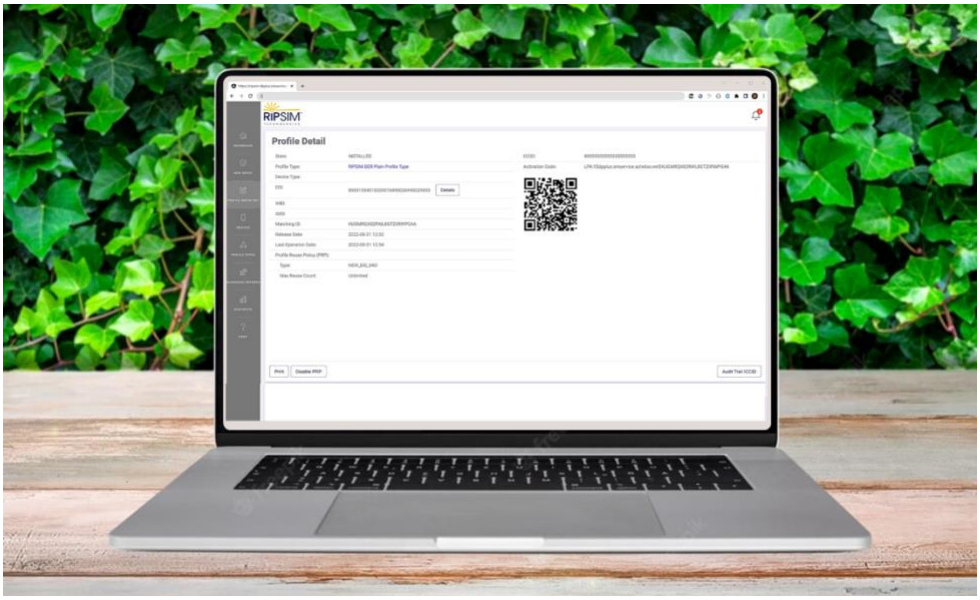

FIGURE 8 - RIPSIM ESIM SECURE ROUTER (SM-DP+)

RiPSIM Software Suite Architecture

The RiPSIM Software Suite is built on a contemporary, micro-services based architecture to give customers maximum flexibility in its deployment and operations. This flexibility allows customers to deploy modules either as cloud native services or as a container cluster deployable by a modern, cloud-native orchestrator. Among others, the RiPSIM Software Suite works in AWS and Microsoft Azure cloud environments which have the GSMA SAS-SM certification of their data centers in various regions.[2] Leveraging the implementation of OpenID for roles access, each element of the RiPSIM Software Suite can be configured to grant access to only those users who are authorized to enter a particular section of the RiPSIM Software Suite. The user interface is a highly intuitive, web-based

[1] Discovery services are offered via the GSMA and Apple's ALS (Apple Lookup Service).
[2] https://www.gsma.com/security/sas-accredited-sites/

application from which the user can create new, or modify existing, profile templates as well as initiate eSIM generation jobs. As shown below, flexible input, HSM, and output adapters have been implemented to readily facilitate integration to existing customer systems, thereby minimizing the need to make IT changes at the customer's side. At the center of the system lies the message broker that facilitates the various components/modules across the platform to pass events and messages to one another. Through this orchestration, the RiPSIM Software Suite will be readily upgradeable to real-time eSIM generation and provisioning as customers deploy this capability.

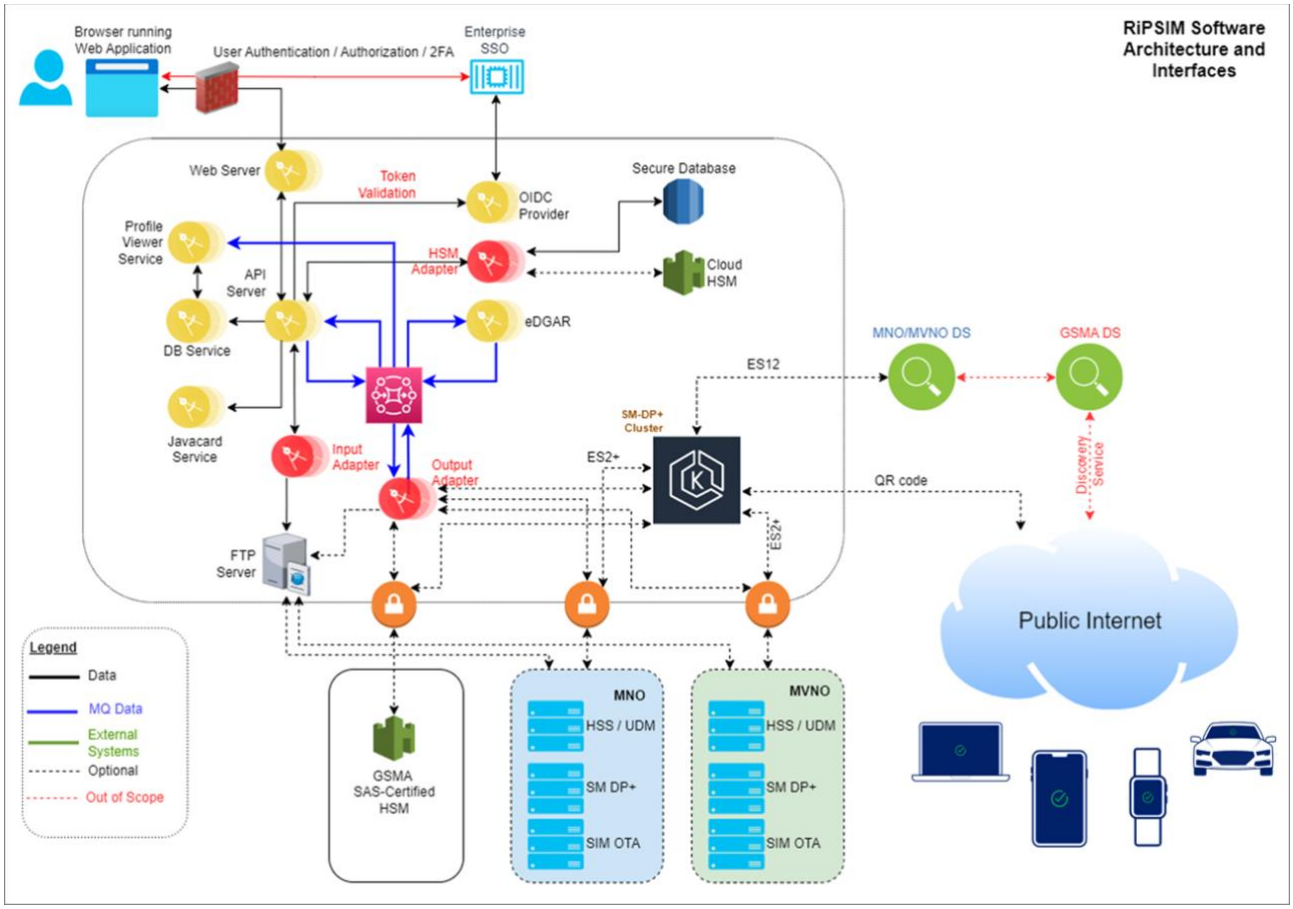

FIGURE 9 - RIPSIM CLOUD NATIVE ARCHITECTURE

Summary

In summary, the RiPSIM Software Suite provides the following:

- **Autonomy:** the RiPSIM Software Suite is an end-to-end eSIM lifecycle management platform that allows you to independently create consumer and M2M/IoT profiles, generate individual eSIMs, and download them to devices in the field.

- **Interoperability:** the RiPSIM Software Suite integrates with existing customer operational and billing support systems and other infrastructure, minimizing the need for any changes in the customer's domain.

- **Scalability:** the RiPSIM Software Suite supports massive scale to allow for the generation and rollout of millions of eSIMs on-demand.

- **Efficiency:** the RiPSIM Software Suite supports customers in real-time, facilitating fast generation of millions of eSIMs within hours.

- **Compatibility:** the RiPSIM Software Suite may be installed in any type of cloud environment (Azure, AWS, Google, etc.) and your eSIMs will work with any type of secure hardware in OEM devices (eUICCs, iUICCs, etc.).

- **Economy:** the RiPSIM Software Suite has a straightforward software subscription model with no superfluous profile, download, or other transaction fees.

- **Security:** the RiPSIM Software Suite complies with or exceeds industry standards and specifications for cloud, eSIM, subscription management, and software security.

Conclusion

The wireless industry is evolving at an accelerating pace giving rise to new technologies that introduce greater operational efficiencies, better security, more flexibility, and disruptive business models. With the eSIM entering mainstream adoption, wireless service providers and enterprise network operators are now free to manage their own eSIM lifecycles without the need to rely on third parties who are often slow, expensive, and inefficient. It is a new era where a wireless service provider can finally have full control of one of its most important security elements: the eSIM.

About RiPSIM Technologies

RiPSIM Technologies has built the first-ever software-defined end-to-end eSIM ecosystem for use by wireless service providers and enterprise network operators in their own cloud environments including Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). Through our patent-pending highly intuitive web interfaces, eSIMs can be fully designed, developed, and seamlessly delivered all from a single platform. And unlike traditional SIM Vendors that rely heavily on a-la-carte pricing models RiPSIM Technologies' platform frees its customers from excessive fees through a simple software licensing model.

RiPSIM Technologies, Inc. is a disruptive software company based in the Washington D.C. metropolitan area that was founded by a team of seasoned professionals with over 175 years of combined wireless experience working across wireless service providers, handset manufacturers, infrastructure, and SIM vendors.

