A Study on Embedded Sims for Machine-to-Machine Remote Provision Connectivity

[1]Devireddy Venkata Manideep, [2]Pavithra H

[1]UG-Student, [2]Assistant Professor,

[1,2]Department of Computer Science,

[1,2]R.V. College of Engineering, Bangalore, India.

Abstract : As the number of connected devices grows, and cellular machine-to-machine (M2M) communications becomes more prevalent, new difficulties emerge that are not present in traditional consumer mobile communications. The usual method of changing a cell provider by switching SIM cards becomes complicated and expensive with extensively deployed M2M devices. To overcome this issue, an over-the-air (OTA) subscription management system known as Embedded SIM (eUICC or eSIM) was created. The eSIM is a novel secure element for managing multiple mobile network provider subscriptions remotely and is compatible with the GSMA's remote SIM provisioning standard. This paper provides a high-level overview of M2M eSIM, and its architecture. The standard sim and eSIM lifecycles are compared. This paper also provides the key features and different compliances for eSIM. It also includes a summary of the challenges and constraints encountered in the field, as well as the present extent of its application in various sectors.

***IndexTerms* - eSIM, eUICC, Internet of Things, M2M, Comparison, Challenges, Applications**

I. INTRODUCTION

Embedded Subscriber Identity Module (Embedded SIM) — An Embedded SIM is a UICC that facilitates over-the-air provisioning of an initial operator subscription as well as future subscription changes from one operator to another in compliance with the GSMA Embedded SIM specification. [1] The use of the GSMA Embedded SIM standards improves industrial and logistical operations for M2M equipment distribution. To comprehend how eSIM technology works in detail, it is required to have a thorough understanding of the technology. This paper's contribution is to analyse eSIM technology for M2M connectivity of IoT devices and present a crucial comparison between regular sim and eSIM throughout their lifecycle. In addition to this, the challenges and applications of eSIM are also highlighted. The paper's structure is organised in this manner. Section II provides an overview of the embedded sims and their characteristics. Section III delves into the architecture of eSIM remote provisioning for M2M communication. Section IV distinguishes between standard sims and eSIMs. Section V describes the various security compliances of the eSIM. Section VI discusses the difficulties encountered in the eSIM. Section VII describes the applications of eSIMs in different sectors. Section VIII contains the paper's conclusion.

II. Overview of Embedded SIMS

On a given mobile network, any SIM card primarily handles authentication, identification, and security through International mobile subscriber identity (IMSI) and Integrated circuit card identifier (ICCID). Before arriving at the eUICC form for usage in IoT and M2M communications, the SIM had gone through multiple iterations, growing smaller with each iteration. With the recent transition from physical SIM to eSIM, the operator's profile and the device’s chipset may now be separable.

The most enticing aspect of eSIMs is the flexibility with which it allows customers to move between MNOs without having to replace physical hardware, due to its over-the-air reprogrammability, and its ability to navigate numerous profiles from various operators on the same device. This, on the other hand, translates into a number of additional features that, in my opinion, have a beneficial impact on the device. Table 1 shows the key features of eSIM.

It should be evident that eSIM entails new business processes in addition to new technologies. Devices can be classified into one of two groups:

Consumer Solution: The end user has direct control over the provider of connectivity and chooses their profile. This design is appropriate for smartphones and tablets, as well as wearables like watches and tiny attached devices like pet trackers.

M2M Solution: IoT device manufacturers and service providers have control over which operator profile is to be sent to the device. This category includes several M2M solutions, such as smart metres and automobiles. [2] The focus of this research is on M2M eSIMs.

Table 1 Key Features of eSIM

	Key Features
Interoperability	The disclosed standards and architecture are anticipated to be followed by all certified partners in the GSMA ecosystem, assuring compatibility.
Flexibility	IoT solution providers can alter device profiles fast and securely with eSIMs. Connectivity adjustments can be done over-the-air or even automatically based on parameters like signal strength, pricing etc.
Power Efficiency	eSiMs use less power than traditional SIM cards, despite the fact that they use cellular connectivity, which is not power-efficient.

III. ARCHITECTURE OF ESIM

The Embedded SIM Specification from the GSMA defines a single, de facto standard methodology for remote provisioning and maintenance of M2M connections, enabling “over the air” provisioning of an initial operator subscription as well as future subscription changes from one operator to another. Figure 1 depicts the architecture of the eUICC remote provisioning system as well as the system interfaces used to carry out the activities.

The following are the main system elements, their interfaces and functionalities:

Subscription Manager Secure Routing (SM-SR):

Operator Profiles and its credentials are prepared, stored, and protected by the SM-DP. It also installs operator Profiles from OTA onto the eUICC.

Subscription Manager Data Preparation (SM-DP):

It will keep track of the status of Profiles on the eUICC and also safeguards the communications link between the SM-DP and the eUICC, which is used to send operator profiles.

Embedded Universal Integrated Circuit Card (eUICC):

The eUICC element is a secure component that allows Subscriptions to be changed. This is not something that can be simply changed or replaced. It incorporates all of the features found in the detachable SIM. [1]

eUICC Manufacturer (EUM):

The eUICC's initial cryptographic setup and security architecture are the responsibility of the EUM. eUICCs are provided by the EUM and include a Provisioning Profile and one or more Operational Profiles.

EUM – SM-SR interface (ES1):

The main function of this interface is to allow the eUICC platform to be registered at the SM-SR.

SM-DP – Operator Interface (ES2):

The Profile ordering elements and techniques are covered by this interface. This interface is also used to download and instal profiles. The SM-DP supplies the operator with the necessary information for the Profiles, allowing the operator to offer the necessary information for the subscription on its mobile network.

SM-DP – SM-SR Interface (ES3):

The interface stores some information about the Profile in accordance with the commercial agreement, operator policy guidelines, and regulatory data retention duties.

SM-SR – Operator Interface (ES4):

This interface is mostly utilised while administering the Profile Lifecycle Management Authorisation (PLMA), allowing M2M service provider to administer a Profile held by an operator on its behalf.

Device – eUICC Interface (ESx):

A Device that has Local Activate / Deactivate capabilities and supports the Emergency Calls can use this interface for creating the Emergency Profiles. When a special Emergency Profile is required, to make Emergency calls, this interface can be used and disabling them after the emergency situation has passed.

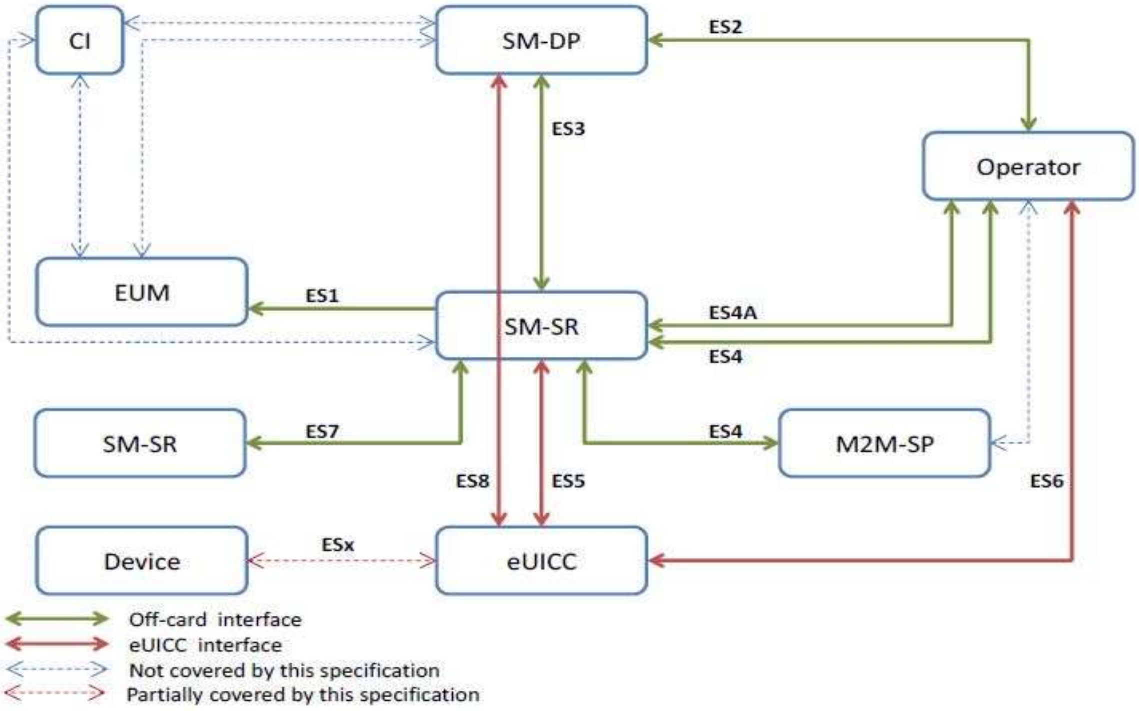


Figure 1 eUICC Remote Provisioning System [3]

IV. Comparison of SIMs

The regular SIM life-cycle and the eSIM life-cycle are compared in Figure 2. The SIM life cycle is altered by eSIM. It shows that eSIM personalisation is separated into two stages. The life-cycle does not follow a linear model beyond the pre-Issuance Part, instead, when a new MNO joins the scene, the eSIM can be provisioned at any moment. As a result, the reusability of an eSIM distinguishes it from a standard SIM. Table 2 shows the comparison of traditional sim and esim.

Table 2 Comparison of traditional sim and eSim [6]

	Key Comparison
Traditional Sim	• It stores a single operator profile and is removable from the device. • If a consumer desires to switch to a different operator, the SIM must be exchanged with the new network provider. • Can cater to all market device categories.
Embedded sim with remote provisioning	• Can store several operator profiles and is incorporated in the M2M device. • If a consumer wishes to move to a new operator, the SIM profile on a deployed SIM can be altered without physically changing the SIM. • If the sim card becomes faulty, the gadget must be replaced entirely. • Designed primarily for remote-access M2M devices, but applicable to other M2M sectors, including wearables.
Removable sim with remote provisioning	• Multiple operator profiles can be stored on a single SIM card while being a detachable piece of hardware. • Remote provisioning allows a customer to alter the SIM profile on a deployed SIM without physically changing the SIM. • If the sim card is broken, it can be replaced without having to replace the complete device. • Currently used in tablets and iPads, but might be expanded to handsets in the future.

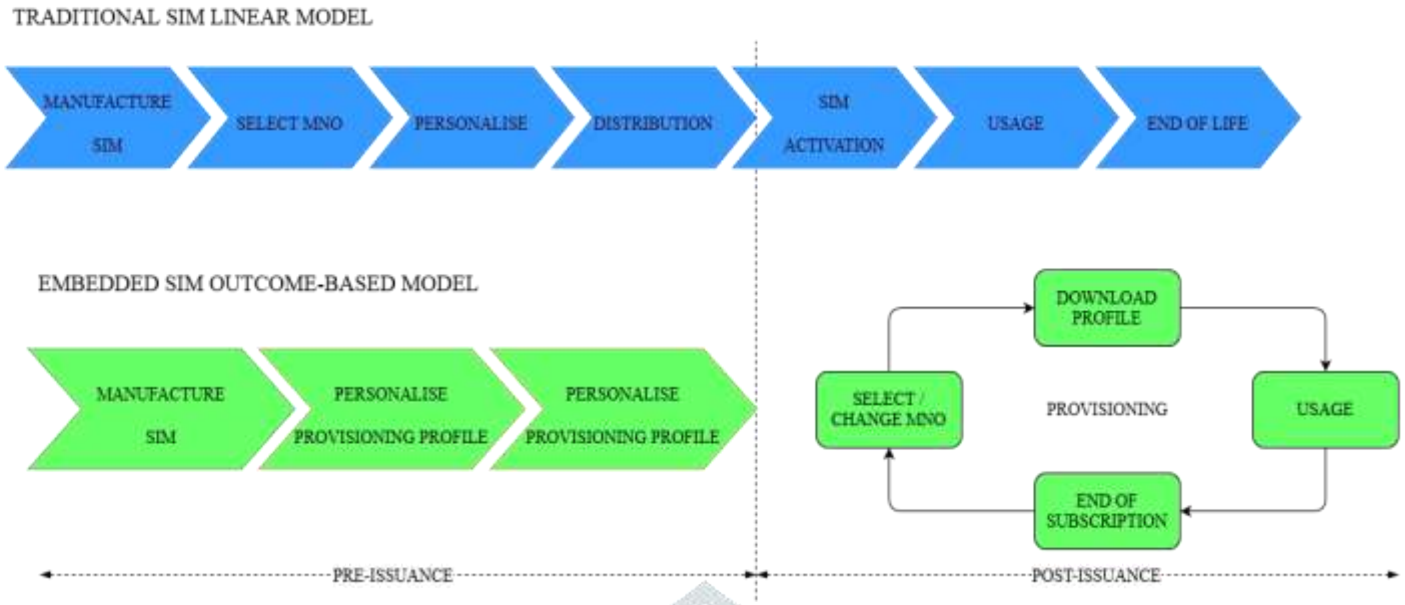


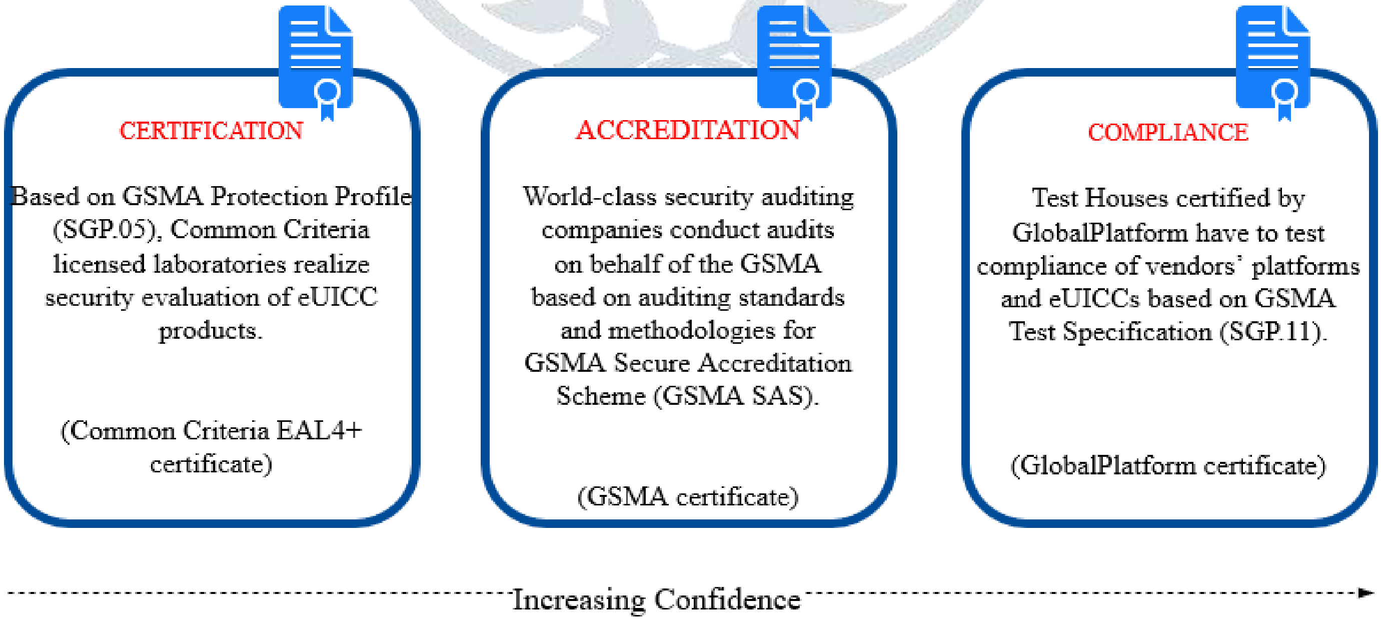
Figure 2: Traditional SIM and eSIM Life Cycle [5]

V. Certifications and Compliance

The GSMA Embedded SIM definition outlines a system that is designed to be reliable, secure, scalable, and interoperable. However, these promises can only be fulfilled if every technology supplier follows the specification in terms of interpretation and implementation. With a multi-layered strategy, compliance is ensured. Embedded SIM manufacturers and subscription managers must submit their devices to a series of tests in order to obtain various certifications that demonstrate compliance. [5] Figure 3 shows different levels of security.

The functional behaviour and interactions with backend servers like the Operator SM-DP and SM-SR are the main focus of the eUICC testing technique. The compatibility of eUICCs with the GSMA requirements is verified using qualified tools. The testing procedure is intended to confirm that the eUICC is functional and interoperable. The software and data installed on the eUICC is tested to verify that it is hack-proof. This "penetration testing" is carried out in specialised security laboratories, with successful goods being certified by national security authorities such as BSI.bund.de.

The testing itself is carried out by Test Houses and laboratories that have been previously accredited and approved by Global Platform. These authorised Test Houses are responsible for a number of important tasks, including provisioning the initial subscription for a new device, testing the provisioning of single and multiple subscriptions, adding new subscriptions or making modifications to existing ones, moving subscriptions, and cancelling them. [5]


CERTIFICATION

Based on GSMA Protection Profile (SGP.05), Common Criteria licensed laboratories realize security evaluation of eUICC products.

(Common Criteria EAL4+ certificate)

ACCREDITATION

World-class security auditing companies conduct audits on behalf of the GSMA based on auditing standards and methodologies for GSMA Secure Accreditation Scheme (GSMA SAS).

(GSMA certificate)

COMPLIANCE

Test Houses certified by GlobalPlatform have to test compliance of vendors' platforms and eUICCs based on GSMA Test Specification (SGP.11).

(GlobalPlatform certificate)

Figure 3 GSMA eSIM Compliance [5]

VI. Challenges And Issues

Despite the fact that eSIM technology has been available for some years, the present eSIM industry is fragmented and fragile, with limited adoption relative to its long-term potential. The key barriers for mainstream eSIM adoption include a diversified IoT market, security concerns, and technological immaturity. This section goes through them in depth.

Reluctance of Mobile Carriers

In order to survive the global adoption of IoT, mobile carriers must rethink their business strategies. However, because the eSIM no longer binds the end-user to a single carrier, carriers are concerned about losing consumers with the click of a button, and the ability to simply change subscriptions (carrier profiles) means consumers will no longer have to pay for pricey roaming. So, the question arises, why should mobile carriers invest in eSIM design when they anticipate more churn and, most likely, no roaming usage? This is also why eSIM adoption has been so delayed.

The trust in Interoperability

Because eSIM is still a relatively new technology, standardising the entire ecosystem is extremely difficult. Although the GSMA has established guidelines for achieving interoperability provided by the eSIM, the true problem comes in its implementation. While migrating to eSIM technology, the telecom sector will go through a series of transitory adjustments. It is nearly hard to get all of the diverse stakeholders together to collaborate without an interoperable solution, especially when trust is already low. Thus, GSMA has placed a high priority on interoperability
problems.

Security

Security is the most serious concern in the world of IoT. Despite the fact that the IoT market has matured sufficiently to address this issue, new technology introduces new security flaws. Because an eSIM is configured remotely, all user credentials are essentially transferred over the air. As a result, side channel attacks are possible against the eSIM architecture. If the hacker is successful in breaking into the connection between the eSIM and the platform, they will have access to actual carrier profiles, which may be exploited in a variety of fraudulent scenarios.

Changing Geographic regulations

Despite the fact that the GSMA governs and ensures the standardisation of Remote Sim Provisioning solutions, it is important to remember that the requirements for hosting a Subscription Management platform and Data-Centers differ per region. This is another large expenditure that entirely eliminates the possibility of using a hosted approach, which is far more flexible.

VII. Applications of eSims

Home security

Sensors are finding their way into smart homes all around the world. Most sensor devices in a house can communicate via Bluetooth, ZigBee, Z-Wave, and other protocols. eSIM technology allows for the delivery of a single home security hub configuration onto any network. A separate cellular-based link to a monitoring provider should be included in a home security hub for increased security. If the homeowner relocates or changes monitoring services, the hub may be easily re-provisioned in a different network. [7]

Automobiles

Instead of outsourcing connections to a specific network provider, manufacturers may manage eSIMs in their vehicles as a managed service, which cuts costs while improving reliability and customer support.

With the eSIMs the automobile drivers experience may be improved through

- collection and transmission of diagnostic data for vehicle servicing,
- critical firmware updates from a car manufacturer,
- emergency call system (eCall),
- monitoring driver behaviour for insurance purposes.

An open ecosystem of diverse connection providers is supported by a fully interoperable and compliant solution of eSims by handling the profile changes through OTA.

Agriculture

To manage facilities, agriculture operations might employ centralised network management. eSIM gives you more control over your cellular-connected devices, making cellular IoT more accessible, inexpensive, deployable, and scalable. Because cellular networks provide such broad coverage, with less cost tracking devices may be used in remote locations and harsh terrain.

One such use case is by using Precision agriculture, which is based on sensor-based real-time crop monitoring and predictive algorithms. We can quickly establish what types of crops should be grown under given conditions using these sensors.

eSIMs that function on the M2M paradigm can be used to link IoT devices that incorporate these sensors.

Table 3 shows the applications and advantages in the specific domains.

Table 3 Application of eSIM

Application	Advantage with eSim
Smart manufacturing	• Reduce waste and speed up production • Improve yield and the quality of goods produced • Achieve better customer satisfaction and brand loyalty
Shipping and logistics	• Ship connected assets anywhere • Connect as a local subscriber on any cellular network • Reduce tracking costs • Avoid physical SIM swapping • Change profiles immediately with RSP
Item tracking and site monitoring	• Reach across geographies • Protect sealed devices against harsh environments • Manage all assets using the same technology • Change profiles with RSP as items move • Reduce potential for tampering
Smart Energy	• Deploy anywhere within cellular coverage • Avoid utility- specific dedicated infrastructure • Register devices securely • Minimize device costs • Manage customer service precisely • Scale service across regions quickly

VIII. CONCLUSION

In this study, we have discussed the building components of embedded sims, as well as a full review of the architecture for M2M IOT devices. In this paper, the traditional and embedded sims, as well as their life cycles, are compared in detail. In addition, the study discussed the problems and concerns that have arisen as eSIM has evolved. This study also covers a variety of eSIM applications in different sectors.

IoT devices are becoming increasingly popular in today's ever-changing technological world. Connected networks, whether wired or wireless, play a significant role in IoT connection dependency. Both of these connectivity requirements can only cover a small number of connections. The network's primary dependence will be eliminated if every IoT device has eSIM technology. The adoption of eSIM technology is not a one-time occurrence; it necessitates a global eSIM infrastructure rollout as well as changes in both technical and business operations.

REFERENCES

[1] GSM Association (GSMA), "eSIM Whitepaper The what and how of Remote SIM Provisioning", pp. 1–21, 2018.

[2] B. A. Abdou, "Commercializing eSIM for Network Operators", In the Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT 2019), pp. **616–621**, **2019**, doi: 10.1109/WF-IoT.2019.8767260

[3] GSM Association (GSMA), "Remote Provisioning Architecture for Embedded UICC Test Specification", pp. **1–452**, **2020**.

[4] GSM Association (GSMA), "Embedded SIM Remote Provisioning Architecture", pp. **1–113**, **2020**.

[5] GSM Association (GSMA), "The importance of Embedded SIM certification to scale the Internet of Things", pp. **1–12**, **2017**.

[6] GSM Association (GSMA), "Analysis Understanding SIM evolution", pp. **1–17**, **2015**.

[7] ARM, "7 Top eSIM use cases Whitepaper", pp. **1–8**, **2019**

[8] A. Sayali Krishna, M. Bhaskar, and T. Surabhi, "eSIM on IoT: An Innovative Approach Towards Connectivity", International Journal of Engineering Research & Technology, Vol. **8**, No. **5**, pp. **1–4**, **2020**.