eSIM Technology and Global Connectivity

Omar Alkhatib, Khaled Zaben, Abdelmajid Bader

Dept of Computer Eng, Princess Sumaya University for Technology (PSUT)

Abstract

Our communication was mostly reliant on physical SIM cards until recently in order to send messages, make calls, and browse the internet via hardware modems. But the physical limits of these physical cards presented challenges. eSIM, a virtual game-changer that is imperceptibly integrated into our devices, enters the picture. It addresses some of the drawbacks associated with physical SIM cards by offering benefits such increased privacy and security in addition to functioning similarly to conventional SIM cards. Looking ahead, new SIM technologies like eSIM appear to be promising and prepared to meet our changing needs. eSIMs are virtual entities that contain cryptographic keys required for authentication and smooth operation in the Subscriber Identity Module (SIM), as opposed to their physical counterparts. This becomes vital, particularly in industries that are fully embracing 5G, where adopting eSIM can greatly benefit from

Keywords: roaming, global connectivity, 5G technology, eSim, cellular wireless communication, and wireless communication.

Introduction

i. Since the 1980s, wireless mobile communication technology has advanced. Since then, there has been an increase in the need and demand for stronger, more potent technology. About once every ten years, a new generation emerges. With its introduction, it resolves issues with its predecessor and introduces fresh technology to improve communication. Finally, we arrive at 5G, our current generation. The goal of the fifth-generation broadband cellular network standard is to ease the overall maintenance and operation of User Equipment (UEs) while also addressing a number of current issues. Increased data rates for high-speed mobility, support for low data rates, low power devices, and robust and strong network security are just a few of the additional criteria it was made to meet. Within 5G Authentication and Authorization Controller's domain (AAC) mechanisms in eSIMs are based on the Authentication and Key Agreement (AKA) protocol [3].

the blazingly fast data speeds. As eSIM becomes more widely used in technology, it could be the solution to end all problems with global connectivity.

This paper delves further into the seamless integration of eSIM with 5G, illuminating the cryptographic elements that are guiding the process. It also begins investigating the fundamental idea that underpins the realization of global connectedness.

ii. The idea behind eSIM cards is to include a conventional SIM card right into the device chip as opposed to attaching it as a separate, detachable component. An actual SIM card does not require to be inserted by users. The electricity equipment can be more effectively managed centrally by utilizing the eSIM card. Simultaneously, it removes the laborious task of manually inserting and withdrawing SIM cards from power equipment [2].

iii. The bond between a standard SIM card and a single mobile provider is one-way; it is as permanent as a tattoo. Imagine the eSIM as the SIM card equivalent of the cool cat. It functions similarly to a permanent SIM

Literature Review

This is how the rest of the document is organised:. We provide a more thorough comparison of eSIMs and conventional SIMs in section (I). The pertinent aspects of 5G, including devices with eSIMs, are covered in section (II). The significance of roaming and worldwide connectivity with future SIM cards (eSIM) is covered in section III. Lastly, we demonstrate a few of the issues that eSIM cards resolved in section (IV).

I. The distinction between an eSIM and a SIM card

Though they do the same tasks and have the same objective, an eSIM and a SIM card that fits into your device without causing any fuss when you take it out, unlike the traditional detachable SIM cards that we are all familiar with. The eSIM truly is revolutionary. You can store numerous mobile operator profiles in the virtual rear pocket of your handset. Get ready for the amazing part: your device can be programmed to remain on a particular profile or to change it at any time, all through over-the-air (OTA) wizardry. This eliminates the need to physically switch SIM cards or go to the store; it's like giving your gadget a stylish makeover without getting up from your couch.

IV. Let's analyze the role that eSIM plays. Imagine it as a three-act drama consisting of machine-to-person (M2P), machine-to-machine (M2M), and a combination of the two. Imagine now that M2P is the environment in which gadgets yearn for human interaction. Imagine the newest technology—laptops, tablets, wearables, and cellphones—being the centre of attention. Now is their chance to shine in the eSIM spotlight.

Enter M2M, an entirely new scene. These are the gadgets that, akin to the unsung heroes of the Internet of Things (IoT), card differ primarily in their provisioning and personalization procedures. In the conventional SIM card scenario, customers sign a contract with the operator of their choice and obtain a physical SIM card. To enable network connectivity, this card is a tangible piece of hardware that you can put in and take out of your device.

In contrast, the eSIM is a smaller piece of hardware that is permanently embedded in your device. To establish network connectivity, the process involves users initiating a contract with their preferred operator. Instead of receiving a physical SIM card, they are provided with an activation code, commonly presented as a QR code. By scanning this QR code using the device, the device initiates the remote download of a profile. Once the profile is successfully downloaded and installed, the device becomes capable of connecting to the network seamlessly.

II. Transfer from SIM to eSIM

Swapping SIM cards is the traditional method of switching mobile operators, but this is a troublesome and costly operation that every company in this industry strongly advises against. This is because doing so ties companies to contracts with operators, which reduces their flexibility. Instead, companies seamlessly establish data connections without requiring human intervention. They are the unseen workers in the backstage area of eSIM.

Now, for the grand finale – the mixed category. It's the ultimate combo, bringing together M2M and M2P. Think of connected cars, stealing the show. While they primarily thrive on M2M communication, they graciously allow human interaction for various services [6]. It's like having the best of both worlds, where the eSIM orchestrates a harmonious symphony between machine and human communication.

v. The GSMA RSP standard defines that the profile (user identity authentication data), epic (card hardware, profile carrier), terminal, eSIM platform (sm-dp+), CI, Discovery Servers (DS), and other supporting facilities are the primary components of the eSIM architecture [12].

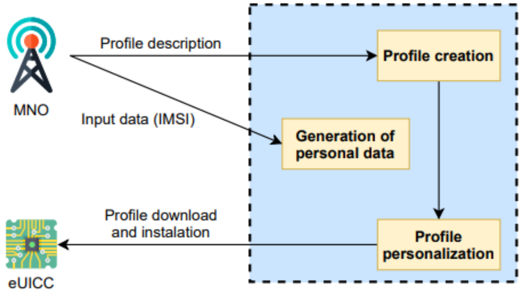
An eSIM, or embedded SIM, is one that is soldered straight into the gadget, enabling the physical chipset and the operator profile to be kept apart. It is currently trending towards more integration with devices, where profiles hold identical data that would have been placed in a standard SIM card, such as a portion of silicon in the System on Chip (SOC) or even often choose to replace outdated devices entirely and time changes to coincide with product releases. The Global System for Mobile Communications (GSMA) created the eSIM standard in order to solve this issue and meet the requirements for scalability, interoperability, and Over-the-Air (OTA) connectivity. SIM cards supply the necessary setup and base authentication material, enabling the devices to be connected to the cellular network [1]. Practically speaking, a SIM card is used by a Mobile Network Operator (MNO) to identify and authenticate a user in order to obtain access to it. As a result, it establishes the contractual relationship between the issuer (MNO) and users. The International Mobile Subscriber Identity (IMSI), which is a number used to identify a SIM card within a network, and the Authentication Key (Ki) are securely stored on SIM cards. It can also store apps and data securely [1].

III. 5G and eSIM

Currently in widespread usage for cellular communication, 5G technology operates in a wide range of environments with multiple sorts of connections, networks, devices, and user interactions. Better software utilisation and programmability also enable a functionality in an enclave. As a result, even if profile and smart cards are different, eSIM and SIM cards serve the same function and are utilised in the same way [1]. But the primary distinction in relevance has to do with how they are provided and tailored. When utilising a physical SIM card, the user signs a contract with the telecom operator and obtains a pre-programmed card from the card stock.

An activation code is provided to the user of an eSIM in lieu of a physical card, although the user still requires a contract with the operator. It allows the user to download a profile that is ready to be placed on the device, which enables the device to establish a network connection.

Figure 1 depicts the actions related to the profile from the description until the download.



wide range of equipment and network functions.

The Authentication and Key Agreement (AKA) protocol, which aims to provide mutual authentication between a UE and the operator, is the foundation for the 5G Authentication and Authorization Controller (AAC) procedures in eSIMs. These methods establish keys to protect subsequent communications [3]. The AAC procedure was predicated on the employment of SIMs as secure elements in earlier network iterations. Together, however, these have made eSIM far more flexible since it enables third parties to select their preferred AAC technique and update such settings virtually instantly without requiring hardware modifications [3].[1]. Additionally, safeguard services that are currently or intend to be offered in the 5G, 4G, and 3G channels as well as the Ka (27.5-29.5 GHz) band [4].

Many of the technological issues that 5G encountered are expected to be resolved in 6G, the upcoming generation. The authors of [9] suggest a strategy that is based on using conventional public-key cryptography in 6G. The authors first examine the possibility of using SIMs to hold cryptographic keys for authentication; however, they also recognise the drawbacks of using physical SIMs and investigate the potential applications of other SIM technologies, such eSIMs. This change is a calculated attempt to improve security and overcome obstacles in the rapidly developing field of telecommunications technologies.

There are a few privacy concerns, nevertheless, that permit 5G device tracking. The eSIM remote management architecture can be employed by the smart grid operator to oversee or implement supplementary services, such as device profiles [16].

IV. global connectivity

Users are only connected to one cell operator with a standard SIM card. The quality and speed of the mobile company's network in a given location determines how well a mobile device performs there. People frequently have to pay their phone carriers a large amount of money for accessing the internet and making calls when using their phones abroad. They take these steps to ensure that their phones function as they would at home.

Issues related to worldwide connection will be permanently overcome once eSIM technology gains traction. Without the need for a physical SIM replacement or a trip to a physical store, users can store multiple mobile operator profiles on the eSIM, a non-removable SIM hardware integrated into the device that can be programmed to use a specific profile or change a profile at any time over-the-air (OTA) [5].

V. eSIM in M2M Communication

Advanced technology known as machine-to-machine (M2M) communication allows systems that are wired or wireless to link as long as they have the same capabilities[19].

This thesis will mostly concentrate on the use of eSIM in consumer It is equally important to talk about eSIM use in M2M applications, since this was the original driving force behind the development of eSIM and remote SIM provisioning. The number of connected devices is rising, and with it is the need for smaller, more manageable devices and an ever-increasing number of energy-efficient devices for Internet of Things use cases.

There are a number of issues with the traditional approach of installing a regular SIM card in these kinds of devices, as [7] explains. Standard SIM cards are limited to one carrier, and in order to change a subscription, the SIM card must be replaced in its whole. This can be a challenging and costly process, especially if the device is located in an inaccessible or remote area. These elements raise the SIM card's production costs and lead times.

Before selecting and provisioning the service straight from the device, users may compare several mobile operators in the area based on factors like price, network speed, and quality. This eliminates the need to visit the neighbourhood cell store or swap out their present SIM card. As an alternative, customers won't have to worry about the underlying mobile network providers when purchasing mobile connectivity from a Smart Global MVNO, which can be an OTT Player (like Amazon, WhatsApp, etc.) or a device maker (like Google, Apple, Samsung, etc.). Mobile providers will compete more as a result of eSIM, which will result in non-committal data plans at affordable prices [5].

Device makers such as Google, Apple, and Samsung can enhance consumer satisfaction by offering device rental plans that include connection, thanks to eSIM. Additionally, they can offer more sophisticated cell plans with value-added services for a premium and free basic connection.

Figure 2: Smart Global MVNO with eSIM Global Connectivity

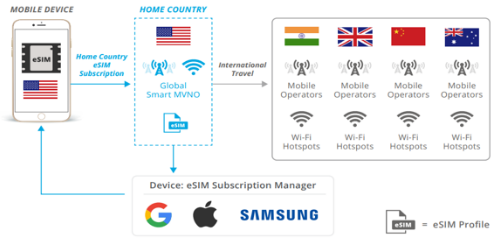
The remotely reprogrammable eSIM and the remote SIM provisioning system were created in order to address all of these various problems [7, 8 Related Work]. Since the eSIM is integrated into the device and cannot be removed, eSIM technology can handle switching subscriptions to a different service provider. Additionally, since eSIMs contain multiple subscription profiles, they enable constant access to the platform or profile for data management, remote updates, and request sending. It's crucial to remember that eSIMs are not limited to smartphones, as this facilitates their integration into Internet of Things devices [10].

Principles of M2M Application is one of the numerous prerequisites for M2M communication. To enable contact with the M2M device or gateway, interaction M2M systems should offer data or information exchange via SMS or IP-based connected services between the devices.

The network is utilised in IoT to enable efficient information flow between linked devices; in M2M, on the other hand, the network might not be employed [18].

VI. GSMA Embedded SIM Project

In the M2M (Machine-to-Machine) space, the GSMA (Global System for Mobile Communications) has developed an



The goal of this is to preserve the degrees of security offered by conventional SIM cards. The ecosystem as a whole is encouraged to follow a single industry standard that permits economies of scale in order to guarantee economic success.

A secure, interoperable architecture is something that the GSMA, SIM makers, and mobile network operators are actively working on. Delivering a unified framework with verified components that provide safe encryption and operator credential transfer is the aim. Solutions that comply with the GSMA Embedded SIM Specification have already been launched or are scheduled to be launched by a number of prominent mobile operators, SIM, and module manufacturers [8].

VII. ESIM Security

Because eSIMs are hardware-based, their security is strong. To be more specific, we're making things nice by using a system-internationally recognised specification for remote over-the-air provisioning and re-provisioning of network operator credentials in partnership with mobile network operators and SIM manufacturers worldwide.

Let's take a closer look at the Remote SIM Provisioning (RSP) ecosystem, which is the larger picture. Ensuring secure distant connection is the primary concern. When combined, these layers provide a strong security framework that thwarts all efforts at unauthorised access and functions like a digital fortress. It provides safe, private, and genuine communications akin to having a guardian shield [10].

However, new technologies also bring with them some security hazards. Some of these vulnerabilities for eSIM are as follows: 1) SIM-Jacking: this is a problem since the operational environment's failure defences could be impacted by an inept log Rhythm AI engine. 2) Privacy Concerns: Service providers are exposed to insider threats and circumstances of personal data leakage during system operations due to the e-SIM system's lack of immediate threat and risk prediction. 3) False Information: Con artists may use false messages purporting to offer support from on-a-chip (SoC) solution that offers an excellent degree of authentication. Algorithms like MILENAGE, TUAK, and CAVE are used to impose mutual authentication between servers and clients. Data confidentiality and integrity are strengthened by cryptographic techniques, such as symmetric (DES, 3DES, AES) and asymmetric (RSA up to 2048 bits) cryptography. The eSIM expands on the features of the conventional SIM card by incorporating the capability to dynamically download authentication data. Secure connection is established using TLS, and parties validate their identities via JSON messages [15]. SCP11a is utilised to secure the eSIM profile. Let's go technical now and talk about the GlobalPlatform Card Specification Amendment F. The HTTP request and response language is used by Internet of Things devices to exchange safe data. Imagine it as a technical discussion where the POST requests intervene to guarantee that requests for single function execution are not only safe but also locked down.

service providers to trick users into falling into financial traps [13].

However, eSIM has its own defences against these kinds of security lapses: 1) Reprogrammable Technological System: Compared to traditional SIM cards, the e-SIM offers higher security because it can be programmed. Instead than being saved on the e-SIM itself, personal information is kept with service providers. 2) Carrier Switching Security: Service providers are advised to monitor the network system and impose security limits, as information theft is acknowledged to occur even with security measures in place. When it comes to assessing and distinguishing between IoT and non-IoT devices, strict guidelines ought to be implemented [13]. 3) Information Theft: Service providers must keep an eye on and enact security measures because e-SIMs, like regular SIM cards, are susceptible to information theft [14].

VIII. Description of eSIM Session Key Agreement Protocol

Since no physical SIM card is necessary, supply chain can also be simplified, leading the way for mobile operators to

Session key agreement is an important step in the eSIM process of putting data securely onto the air card. Its primary responsibility is to ensure the security of the configuration files during transfer between SM-DP and ISD-R. Now, before creating each session key, SM-DP gets work generating a new set of temporary public and private keys to keep things interesting.

This is where the eSIM's ECASD comes into play; it sends a random challenge to confirm that the SMDP is who it says it is. Now, the SM-SR has an easier job as a reliable mediator for authentication in secure routing. It passes communications and verifies that all parties are in agreement, but it skips over the specifics of the authentication procedure and uses those arbitrary challenges [17]

You can catch a glimpse of this session key agreement dance in action in Figure 3.

become “Digital Mobile Operators (DMOs)” with limited or no physical presence. Customer service can also be extensively automated with Robotic Process Automation (RPA) and Machine Learning (ML) to reduce the cost of operations further

X. Discussion:

As we considered the significant implications of eSIM technology in the context of telecoms, we talked about how it has revolutionized the way that we restructure global connectivity paradigms, strengthen security protocols, and easily adjust to the ever-changing landscape of mobile communication. Our investigation brought to light the importance of cooperative industry initiatives and the development of standard operating procedures, highlighting the critical role that eSIM technology will play in forming a future in which telecommunications thrive with increased efficiency, adaptability, and interconnectivity among various devices and networks.

XI. Conclusion:

To sum up, this thorough examination of eSIM technology, especially in relation to 5G integration, illuminates its revolutionary influence on international connectivity, telecommunications, and security. The paper

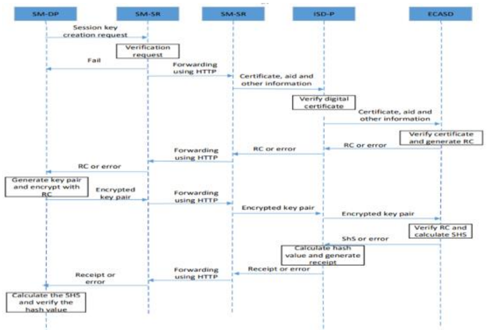

SM-DP
SM-SR
SM-SR
ISD-P
ECASD
Session key creation request
Verification request
Fail
Forwarding using HTTP
Certificate, aid and other information
Verify digital certificate
Certificate, aid and other information
Verify certificate and generate RC
RC or error
RC or error
Forwarding using HTTP
RC or error
Generate key pair and encrypt with RC
Encrypted key pair
Forwarding using HTTP
Encrypted key pair
Encrypted key pair
Verify RC and calculate SHS
ShS or error
Calculate hash value and generate receipt
Receipt or error
Forwarding using HTTP
Receipt or error
Calculate the SHS and verify the hash value

Figure 3: Session key agreement process

IX. Advantages and Disadvantages related to eSIM:

Mobile operators have been at the center of Mobile Industry value chain for a long time, raking significant revenues from device sales, International Direct Dialing (IDD), international roaming, data, voice, and messaging services. With the ascent of OTT players over the last few years, voice, messaging, IDD, and international roaming revenue have been significantly reduced. eSIM has the potential to make device manufacturers the center of the Mobile industry value-chain, leading to mobile operators losing a direct relationship with the customer. In the short term, mobile operators can significantly benefit from eSIM growth as remote provisioning reduces the requirement for physical stores, leading to significant cost savings.

explains how eSIM introduces a paradigm change with improved usability, privacy, and security by eliminating the drawbacks of conventional physical SIM cards. In addition to addressing issues related to mobile operator transitions, the smooth transition from SIM to eSIM and its capacity to support various operator profiles pave the way for dynamic connection in the 5G era.

References

[1] C. Silva, A. Alves, and J. Rodrigues, “eSIM suitability for 5G and B5G enabled IoT verticals,” presented at the 8th Intern. Conf. on Future Internet of Things and Cloud (FiCloud), Rome, Italy, Aug. 2021, pp. 153-158.

[2] Y. Fu, X. Zhang, and Z. Yang, “Terminal access method of power equipment based on eSIM in WSN environment,” presented at the 3rd Intern. Conf. on Power and Renewable Energy (ICPRE), Chengdu, China, Sep. 2018, pp. 1-5.

[3]A. Al Mousa, M. Al Qomri, S. Al Hajri, and R. Zagrouba, “Utilizing the eSIM for public key cryptography: a network security solution for 6G,” presented at the 2nd Intern. Conf. on Computer and Information Sciences (ICCIS), Riyadh, Saudi Arabia, Oct. 2020, pp. 1-6.

[4] H. Jo, J. Kim, and J. Lee, “Methods to evaluate and mitigate the interference from maritime ESIM to other services in 27.5-29.5 GHz band,” presented at the 2018 Intern. Conf. on Information and Communication Technology Convergence (ICTC), Jeju Island, South Korea, Oct. 2018, pp. 675-680.

[5] Sehgal, R. and Sanjib, S., 2018. eSIM-Gateway to Global Connectivity..

[6] Fridh, A., 2020. eSIM Re-Selling on Mobile App.

[7] Meyer, M., Quaglia, E.A. and Smyth, B., 2019. An Overview of GSMA's M2M Remote provisioning specification. arXiv preprint arXiv:1906.02254.

[8] GSMA embedded sim specification - a single common and global specification to accelerate growth in m2m. Date Views 01.03.2020 www.gsma.com/iot/wpcontent/uploads/2014/10/GSMA-Embedded-SIM-Specification-flyer.pdf.

[13] A. R. Mathew, “Threats and Protection on E-sim: A Prospective Study,” in *Novel Perspectives of Engineering Research*, vol. 8, pp. 76-81, Mar. 2022, doi: 10.9734/bpi/rtcams/v8/1907B.

[14] C. Gaber and P. Kaluza, “eSIM Adoption : Essential Challenges On Responsibilities Repartition,” in *2022 1st International Conference on 6G Networking (6GNet)*, pp. 1-6, Jul. 2022, doi: 10.1109/6GNet.2022.9830443.

[15] X. Ren, Z. Yue and Z. Li, “Security system of Internet of Things based on Subscriber Identity Module,” in *Journal of Physics: Conference Series*, vol. 1972, no. 1, pp. 012004, 2021, doi: 10.1088/1742-6596/1972/1/012004.

[16] R. Borgaonkar and M. G. Jaatun, “5G as an Enabler for Secure IoT in the Smart Grid: Invited Paper,” in *2019 First International Conference on Societal Automation (SA)*,

[9] Al Mousa, A., Al Qomri, M., Al Hajri, S. and Zagrouba, R., 2020, October. Utilizing the eSIM for public key cryptography: A network security solution for 6G. In 2020 2nd International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

[10] I. M. Alshenaifi, E. U. H. Qazi, and A. Almorjan, “IoT Forensics: Machine to Machine Embedded with SIM Card,” in *20th International Conference on Information Technology-New Generations (ITNG)*, 2023, pp. 1-6, doi: 10.1007/978-3-031-28332-1_16. sec

[11] M. Meukel, M. Schwarz, and M. Winter, “E-SIM for consumers—a game changer in mobile telecommunications,” *McKinsey & Company*, 2016, pp. 1-8

[12] X. Wang, Z. Li, and J. Gao, “A Scheme for Distribution Automation Terminal Design Based on ESIM,” in *20th International Conference on Information Technology-New Generations (ITNG)*, 2023, pp. 1-6, doi: 10.1088/1742-6596/2476/1/012061.

2019, pp. 1-6, doi: 10.1109/SA47432.2019.8938064 .

[17] Ding, Z., Hu, Y., Luo, W., Huang, Z., Xue, J. and Qin, Z., 2021, October. Formal Analysis and Verification of Embedded SIM Session Key Agreement Protocol. In Proceedings of the 2021 5th International Conference on Electronic Information Technology and Computer Engineering (pp. 882-888).

[18] Pradhan, D. and Tun, H.M., 2022. Security Challenges: M2M Communication in IoT. Journal of Electrical Engineering and Automation, 4(3), pp.187-199.

[19] Farooqi, N., Gutub, A. and Khozium, M.O., 2019. Smart community challenges: enabling IoT/M2M technology case study. Life Science Journal, 16(7), pp.11-17.

[20] A. K. Atabekov and K. S. Duisbekova, “Analysis of eSIM technologies and Wi-Fi offloading algorithms,” *Advanced Technologies and Computer Science*, vol. 2, no. 4, pp. 4-7, 2020