Public Key Cryptography in 6G using eSIM

A SEMINAR REPORT

Submitted by

RESHA CHERIYIL RASHEED

KGR19CS060

to

The A P J Abdul Kalam Technological University

in partial fulfillment of the requirements for the award of the Degree

of

Bachelor of Technology

In

COMPUTER SCIENCE AND ENGINEERING

DEPT. OF COMPUTER SCIENCE & ENGINEERING

COLLEGE OF ENGINEERING KIDANGOOR

DEC 2022

VISION AND MISSION OF COLLEGE

VISION

To be a leading engineering institution in the region, providing competent professionals, who engage in lifelong learning, driven by social values.

MISSION

To prepare engineering graduates for the development activities of the society and industry, and to prepare them for higher engineering education.

VISION AND MISSION OF DEPARTMENT

VISION

To become a center of excellence in Computer Science and Engineering imparting quality professional education to develop competent professionals with social values who are capable of life long learning.

MISSION

To impart quality technical education to students at undergraduate level through constant knowledge upgradation by maintaining pace with the latest sophisticated innovations , research development and industry interaction in the field of Computer Science and Engineering with focus on lifelong learning for the well-being of the society.

Program Educational Objectives (PEO)

PEO1- Have sound knowledge and technical skills required to remain productive in the field of Computer Science and Engineering.

PEO2- Be efficient team leaders, effective communicators and successful entrepreneurs.

PEO3- Resolve technical problems with a positive outlook towards well-being of the society.

PEO4- Function in diverse environments with the ability and competence to solve challenging problems.

PEO5- Pursue lifelong learning and professional development through higher education.

Program Specific Outcomes (PSO)

PSO1- Ability to appreciate, learn and develop applications using modern programming languages, and databases.

PSO2- Ability to understand and analyze computer networks, distributed systems and computer system architectures for the designing of new systems.

PSO3- Ability to apply knowledge of domains like machine learning, cloud computing , image processing, data mining and software engineering to tackle innovative problems

DECLARATION

I undersigned hereby declare that the seminar report "Public Key Cryptography in 6G using eSIM", submitted for partial fulfillment of the requirements for the award of degree of Master of Technology of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of Mrs. Shandry K K. This submission represents my ideas in my own words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Kidangoor

03-01-2023

RESHA CHERIYIL RASHEED

DEPT. OF COMPUTER SCIENCE & ENGINEERING

COLLEGE OF ENGINEERING KIDANGOOR

2022-23

CERTIFICATE

This is to certify that the seminar entitled **"Public Key Cryptography in 6G using eSIM"** submitted by **Resha Cheriyil Rasheed (KGR19CS060)** to the APJ Abdul Kalam Technological University in partial fulfillment of the award of B.Tech degree in Computer Science and Engineering is a bonafide record of the seminar carried out by me under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Mrs. Shandry K K
Assistant Professor
Dept. of CSE
Seminar Guide

Mrs.Mary Priyanka K.S
Assistant Professor
Dept. of CSE
Seminar Coordinator

Dr. Ojus Thomas Lee
Associate Professor
Dept. of CSE
Seminar Coordinator

Mrs. Jyothis Joseph
Assistant Professor
Dept. of CSE
Head of the Department

ACKNOWLEDGEMENT

I wish to acknowledge all those who helped me to complete this seminar. Firstly, I thank the Almighty for helping and guiding me with his light in the right path to accomplish this.

I wish to express my sincere thanks to **Dr. B. V Mathew**, Principal, College of Engineering Kidangoor for providing all the necessary facilities and support.I extend my sincere gratitude to **Mrs. Jyothis Joseph**, Head of Department, Computer Science and Engineering, for her constant motivation and support. I'd take this opportunity to express my profound gratitude and deep regards to our seminar coordinator **Mrs. Mary Priyanka K.S**, Assistant Professor, Computer Science and Engineering.

I am obliged to all the faculty members of our department for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of this assignment. Lastly, I thank my family and friends for their constant encouragement without which this seminar would not be possible.

Resha Cheriyil Rasheed

ABSTRACT

The future brings a whole suite of technical challenges that are no match for the current standard, 5G. Therefore, those challenges must be resolved by the next generation, 6G. Although features such as extremely high data rate is important, it is even more important to plan the security at this phase.

In this seminar, we propose to use traditional public key cryptography in 6G instead of experimental technologies such as quantum communications, artificial intelligence, or blockchain. We do so by utilizing the subscriber identity module (SIM) to store the cryptographic keys needed for authentication.

While the capabilities of current SIMs are limited by their physical attributes, future SIM technologies such as eSIM show great promise to enable sufficient resources for our scheme as they are virtual.

The proposed scheme is simpler, easy to implement, requires no third party, cost effective, and utilizes algorithms that have proven their security for decades.

List of Figures

Contents

Chapter 1

Introduction

Wireless mobile communication technology has been developing since 1980s. Since then, the demands and needs for a better, more capable technology has been rising. New generation arrives roughly each 10 years. With its arrival, it overcomes challenges faced with its predecessor and brings new technologies to facilitate communications. Which brings us to our current generation, 5G. Although it supports incredibly high data rate, low latency, and many other features, it is nowhere near the needed requirements for the foreseen future.

With the state of Internet of things (IoT) being a reality, and the concept of smart cities is no longer a part of science fiction, we realize that current state-of-the-art network technologies will not be sufficient to transfer data within a timely manner. Cities like NEOM are a prime example of what the future might look like and what technical challenges lies ahead. Such future requires robust infrastructure with immense quality of

service (QoS). Currently, the cutting-edge mobile technology is 5G. While it supports incredible speeds, it would still be insufficient to drive the amount of data required in the inevitable age of smart cities. Therefore, the need for a new technology is emphasized.

In response, researches had already began working on a new standard, beyond 5G (B5G), 5G+, or 6G. While the new standard overcomes most of the QoS limitations of 5G, it has to ensure security as it's critical in a such highly interconnected environment. It is especially important that we plan the security in the early phases such as now.

Chapter 2

Background

To better understand 6G, we will briefly go through its previous iteration, as knowing the current state of wireless mobile communication technology will help us understand 6G better. The fifth and current cutting-edge of wireless and mobile technology is yet to be fully rolled-out. Only a handful of ISPs have support for this standard around the globe because it requires complex infrastructure.

5G is characterized by its 3 main services. Enhanced mobile broadband (eMBB), massive machine type communication (mMTC), and ultra-reliable low latency communications (uRLLC). eMBB allows 5G to supports data rates of up to 10 Gbps [15]. mMTC provides Internet access for monitoring and sensing devices, including IoT devices. uRLLC enables the ability for remote surgeries and autonomous vehicles at latencies as low as 5 ms with 99.999 percent reliability.

On terms of authentication, 5G uses EAP-AKA protocol. Although EAP-AKA is robust and resilient, there were concerns regarding its performance. He noted that if the authentication happens frequently, the network may suffer from congestion that results in a high authentication delay.

In telecommunications, 6G is the sixth generation mobile system standard currently under development for wireless communications technologies supporting cellular data networks. It is the planned successor to 5G and will likely be significantly faster.Like its predecessors, 6G networks will probably be broadband cellular networks, in which the service area is divided into small geographical areas called cells. Several companies like Airtel, Apple, Ericsson, Jio, LG etc and research institutes (Technology Innovation Institute) and countries like United States, China, India, Japan and so on have shown interest in 6G networks.

6G networks are expected to be even more diverse than their predecessors and are likely to support applications beyond current mobile use scenarios, such as virtual and augmented reality (VR/AR), ubiquitous instant communications, pervasive intelligence and the Internet of Things (IoT).It is expected that mobile network operators will adopt flexible decentralized business models for 6G, with local spectrum licensing, spectrum sharing, infrastructure sharing, and intelligent automated management underpinned by mobile edge computing, artificial intelligence (AI), short-packet communication and blockchain technologies.

Chapter 3

About 6G

Despite the fact that 5G is still not fully rolled-out and gained popularity, researches have already begun working on the next standard, which is expected to commercialize sometime in 2030.According to many literatures, united views on some of its characteristics are as follows:

3.1 Very High Data Rates

6G will be deployed in smart cities where the data rate must be astronomical in order to accommodate its environment's needs. Literatures have suggested peak data rates of up to 1 Tbps.

In order to achieve such data rates, few things have to change regarding our infrastructure. First, 6G has to operate at a frequency of 1 THz. This creates several challenges since operating at such high frequencies requires special hardware. Because of the extremely small wavelength, we

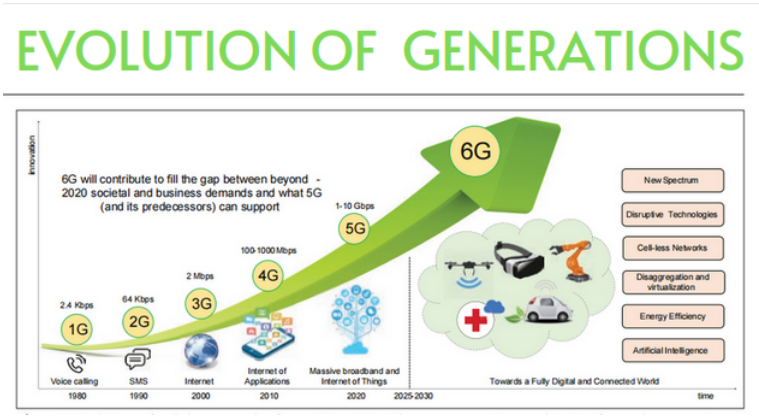

Figure 3.1.1: *Evolution of cellular networks, from 1G to 6G, with a representative application for each generation.*

will need new designs for highly dense antenna arrays.

Consequently, by using such complex antenna set up, sniffing the THz traffic or intercepting it would become much more difficult, thus making it more secure. However, such set up will not completely eliminate eavesdropping. As such, new countermeasure for THz eavesdropping is required.

3.2 Machine Learning Capability

6G will be deployed in a challenging environment. Therefore, artificial intelligence (AI), and particularly machine learning (ML) will be utilized to resolve those challenges.It could be used to intelligently allocate optimal bandwidth for each base station or user, and it can also choose the best possible way to transmit the data between the base station and the

user, which will result in a better user experience

Furthermore, AI can provide better security if utilized properly. By using AI to choose a fitting security algorithm, it will reduce the security overhead regarding data transmission, especially with short packets such as those found in IoT context.

3.3 Ultra-Reliable, Low-Latency Communications

6G will be deployed in a highly challenging environment where few milliseconds of delay may be the difference between life and death. To accommodate such scenarios, 6G will have a sub-millisecond latency, others even suggested latencies as low as 10 to 100 μs. Furthermore, 6G will support extremely high mobility. Handoff will be possible at speeds of more than 1000 km/h, which will be needed for some cases such as airline systems.

Further, in some cases where extreme reliability is required such as industrial controls, 6G will offer low latency communications where the error rate is as low as 10- 9 or 1 bit for each Gb.

3.4 Network Security

Network security in 6G is arguably the most difficult part about its design. Designing a scheme that handles massive amount of stations at an insane data rate with minimal error rate while maintaining security is not a trivial task. To overcome those challenges, some suggested the possibility of

a blockchain-based authentication that is scalable and decentralized, which is suitable for environments such as smart cities.

New technologies such as eSIM eliminates the need for a physical SIM card, including all of its hardware limitations. This means that the SIM will entirely be software-based, i.e. virtual, which opens for a lot of possibilities. Previously, what you can store on the physical SIM is largely limited by its storage capabilities. However, since the eSIM is virtual, the capabilities of the eSIM is as good as the mobile device, which tend to have decent storage and processing capabilities. This allows us to store large key (e.g. 8192-bit RSA keys) that would otherwise be impractical to store on a traditional physical SIM. We see this as an opportunity to introduce a more secure and well-known architecture instead.

Chapter 4

What is an eSIM

An eSIM (embedded-SIM) is a form of programmable SIM card that is embedded directly into a device. Instead of an integrated circuit located on a removable universal integrated circuit card (UICC), typically made of PVC, an eSIM consists of software installed onto an eUICC chip permanently attached to a device. to register new number and sim on device.

Figure 4.0.1: *eSIM Logo*

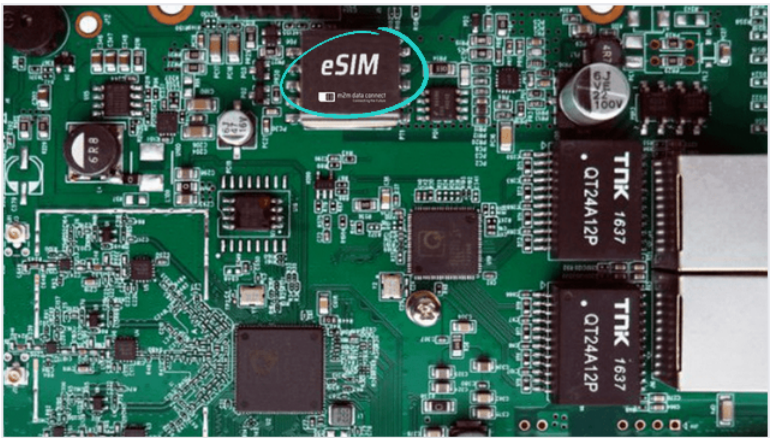

Figure 4.0.2: *eSIM on Motherboard*

eSIM's are embedded in cellphones right from manufacturing process. eSIM is the hardware component that can be soldered and eUICC is the software component.Enables provision for multiple profiles in the mobile. Scan QR code to register new number and sim on device.

Once an eSIM carrier profile has been installed on an eUICC, it operates the same as a physical SIM, complete with a unique ICCID and network authentication key generated by the carrier. The eSIM standard was first released in 2016; since that point, eSIM has begun to replace physical SIM in domains including cellular telephony.

An eSIM is typically provisioned remotely. All eSIMs are programmed with a permanent eSIM ID at the factory. This number is used by the provisioning service to associate the device with an existing carrier subscription and to negotiate a secure channel for programming.

4.1 Design

A traditional SIM card consists of an integrated circuit located on a universal integrated circuit card (UICC), typically made of PVC, which is manually inserted into a device. By contrast, an eSIM is a virtualized SIM card profile installed onto an eUICC chip permanently surface-mounted to a mobile device at the factory. The eUICC chip used to host the eSIM uses the same electrical interface as a physical SIM as defined in ISO/IEC 7816. Once an eSIM carrier profile has been installed on an eUICC, it operates the same as a physical SIM, complete with a unique ICCID and network authentication key generated by the carrier.

4.2 eSIM Architecture

With Remote SIM Provisioning, there are no traditional SIM cards1 . Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card.

Remote SIM Provisioning for the M2M model utilises a server driven (push model) to provision and remotely manage operator Profiles. The solution is organised around 3 elements: the SM-DP (Subscription Manager - Data Preparation), the SM-SR (Subscription Manager - Secure Routing) and the eUICC.

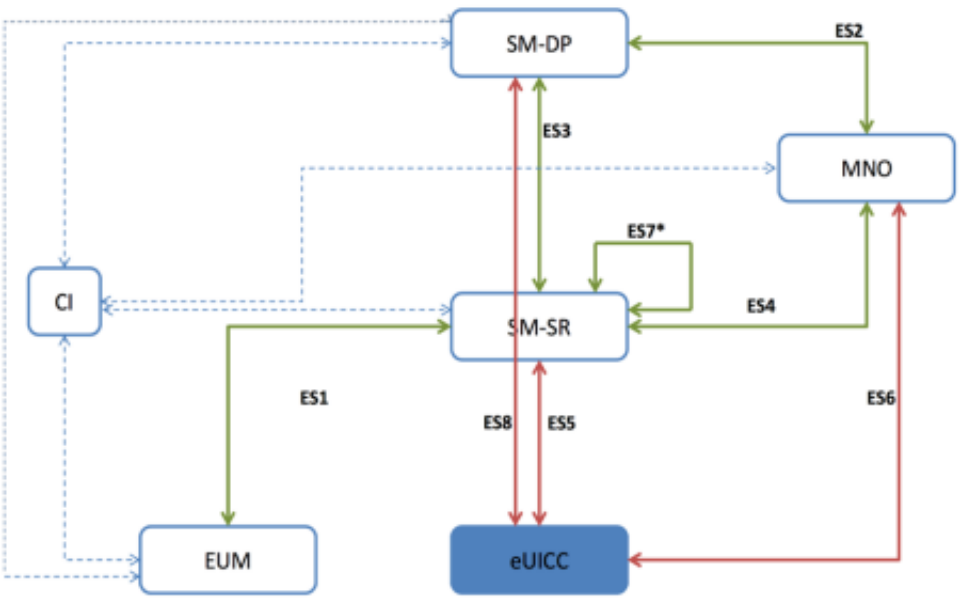

Figure 4.2.3: *eSIM M2M Architecture*

The diagram below is the high-level representation of the M2M main system elements. Beyond common SIM functions, such as SIM Toolkit6 and Bearer Independent Protocol (BIP7) support, the M2M solution does not impose additional requirements on M2M devices to enable usage of eUICCs.

4.2.1 SM-DP

The SM-DP is responsible for preparing, storing and protecting operator Profiles (including the operator credentials). It also downloads and install Profiles onto the eUICC.

4.2.2 SM-SR

The SM-SR is responsible for managing the status of Profiles on the eUICC (enable, disable, delete). It also secures the communications link between the eUICC and SM-DP for the delivery of operator Profiles.

4.2.3 eUICC

The eUICC is a secure element that contains one or more subscription Profiles. Each Profile enables the eUICC to function in the same way as a removable SIM issued by the operator that created it. An eUICC may be built using any form factor from the traditional removable card to embedded formats soldered into devices.

Chapter 5

Utilizing eSIM for Public Key Cryptography: A Network Solution for 6G

The core and essence is that we can, and should, use public key cryptography using keys stored in the eSIM. This opens the door for many possibilities. For instance, we may choose to establish a full public key infrastructure (PKI) without the need for a certificate authority (CA) or any other third party. This can be done by allowing the service provider (SP) to generate public and private keys for each eSIM. The SP should only store the public key of the eSIM card and never the private key

Keep in mind that, unlike traditional public keys, the public key of the eSIM should be securely kept hidden and never to be exposed to the

public as it would compromise the security of our scheme. Furthermore, the SP will also have a public and private key, and the SP will ensure that every eSIM it produces has its public key hardcoded. This is similar to how web browsers have the public keys of CAs hardcoded to prevent spoofing. Now that both parties know each other's keys, any asymmetric cryptographic operation is possible, including authentication.

5.1 Example of an Authentication Scheme

We will show an example of cryptographic operations that can be performed using our approach that ensures both authenticity and confidentiality.

Fig. 5.1.1 and 5.1.2 depicts a scheme using our approach. The first step is the user equipment (UE) requesting access by sending a probe request to the base station (BS). Then, the BS station will send a response requesting for the client's identity. In addition, it will include a sequence number to prevent replay attacks.

After that, the UE will attempt to prove its identity. It will do so by appending the international mobile subscriber identity (IMSI) with the sequence number given by the BS. The output will then be encrypted using the private key of the eSIM which is obtained by the SP when the eSIM was manufactured. This is similar to digital signature, and it is done in order to ensure the authenticity of the UE. After that, it will encrypt it again, but with the public key of the SP instead. This step is to ensure that

no one except for the SP will be able to decrypt it, which in return ensures mutual authentication. After that, the client will append a cleartext IMSI to the encrypted message that contains the IMSI and the sequence number. Then, itsends it to the BS.

The reason behind appending the cleartext IMSI is to allow the authentication center (AuC) to retrieve the corresponding public key of the eSIM in order to successfully decrypt the message and verify the authenticity of the UE.

After that, the SP will receive the cleartext IMSI and the encrypted message containing the IMSI and the sequence number. Then, the SP will decrypt the message using its private key. If a malicious BS that is pretending to be the legit SP is attempting to associate with the UE, it will fail to decrypt the message as it does not have the private key of the legit SP. After that, the AuC will search for the public key associated with the IMSI.

After finding the public key of the eSIM, the SP will decrypt the message once again, this time using the public key of the eSIM. Once done, the SP will have the sequence number and the IMSI. The SP can now verify the sent sequence number with the decrypted sequence number. If the verification fails, it means that the UE might be trying to perform a replay attack. In addition, if the decrypted IMSI is not equal to the plaintext IMSI sent by the UE, it means that the UE might be trying to spoof its identity.

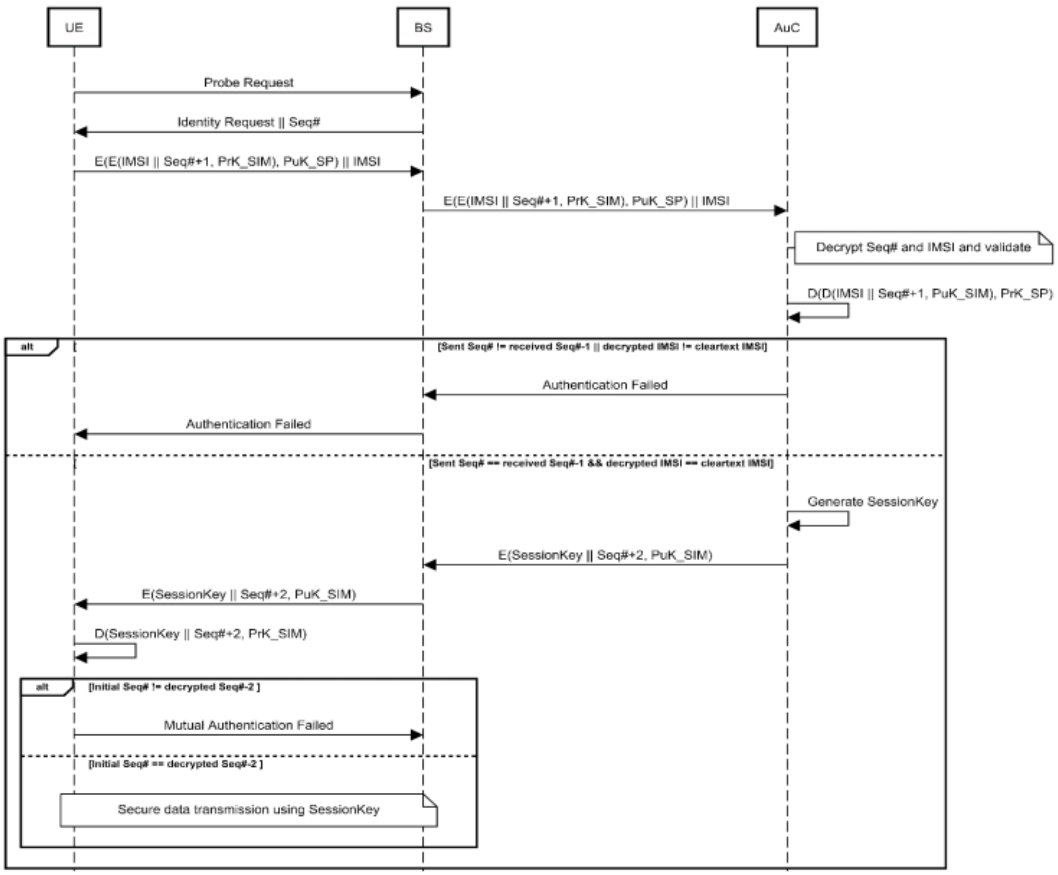

Figure 5.1.1: *Sequence diagram of an example scheme utilizing our approach*

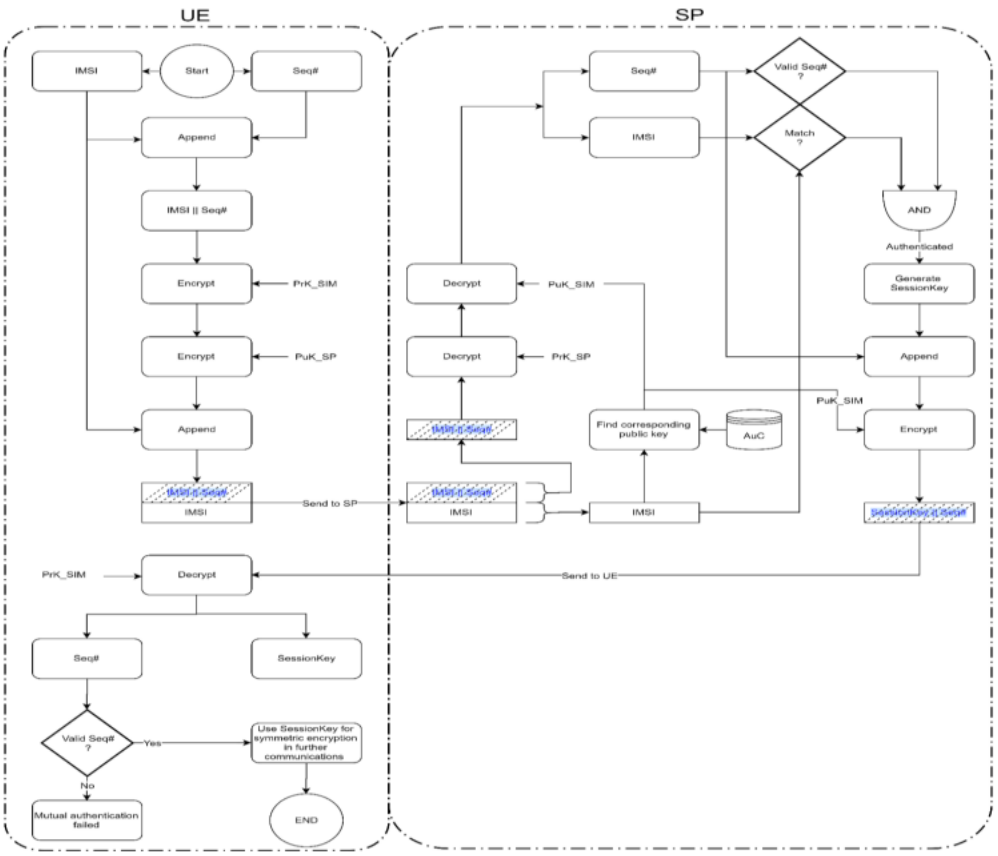

Figure 5.1.2: *Flow chart of an example scheme utilizing our approach*

On the other hand, if the sequence number is successfully verified and the decrypted IMSI is equal to the plaintext IMSI, the UE is to be authenticated successfully. After that, the session key is generated and encrypted with the sequence number using the public key of the eSIM in order to prevent sniffing. The session key is generated to be used for symmetric encryption in further communications as it is more efficient in that regard.

As a final step, the UE will decrypt the message sent by the BS that contains the session key and sequence number. After that, the UE will verify the sequence number as if it's not valid, it means that the BS might be malicious. However, if it's valid, the UE may use the provided session key for symmetric encryption in further communications.

5.2 Attacking our Authentication Scheme Example

After explaining our example scheme, we will demonstrate how an attacker might try to attack it. By doing so, we are testing and proving the security of our proposed solution.

5.2.1 Replay Attack

Let's assume that an attacker, Eve, is listening to the communication between Alice (UE) and the BS, and Alice has successfully authenticated itself. Eve will be able to capture the identity request and sequence number that issent from BS to Alice, and the encrypted sequence number and IMSI appended to a cleartext IMSI which is sent from Alice to BS.

After Eve has successfully captured the aforementioned information, she will attempt to perform a replay attack. First, she will send a probe request to the BS. After that, she will receive the identity request and a sequence number. Then, she will send the previously captured information in hope to be authenticated. The SP will decrypt the message that contains the IMSI and the sequence number.

After that, it will validate the decrypted sequence number with the received one. Given that the BS generates random sequence number for each probe request, the sequence number sent by Eve will be different than the one sent by the BS. Therefore, the BS will detect the attack and will not

authenticate Eve. Subsequently, the attack fails.

5.2.2 Man-in-the-Middle Attack

Man-in-the-Middle (MITM) attack is probably one of the most dangerous attacks that can be performed in a network environment. Therefore, it is understandable that any security scheme should protect against such type of attacks. We will demonstrate how Eve might try to perform MITM attack and how the scheme will protect against her.

First, Eve will purchase a fake BS that she has complete control over it. After that, she will spoof the identity of the legit SP and announce itself to have strong signal, and then she waits for victims to associate. Alice, unaware of the legitimacy of the nearby BS, will send a probe request to Eve's BS as it (allegedly) has the strongest signal. After that, Eve's BS will send identity request and a sequence number, just like how a legit BS would. Alice will then encrypt its IMSI and the sequence number using the private key of its eSIM and the (hardcoded) public key of the legit SP, respectively. Then it will send it to Eve's BS. After Eve's BS receives the encrypted message, it finds itself unable to decrypt it as it does not have the private key of the legit SP that is needed for the decryption process. Therefore, the MITM attack fails.

However, what would happen if Eve's BS ignored the encrypted message and claimed that Alice has been authenticated successfully? Well, in that case, Eve's BS would have to generate the session key and append

the valid sequence number to it and encrypt it using the public key of Alice. Unfortunately for Eve's BS, it does not have the valid sequence number nor the public key of Alice. Subsequently, the attack fails again.

5.2.3 Spoofing Attack

One of the most prominent attacks in networks security is spoofing attacks. Which is to falsely identify as another person or software to gain an unauthorized access accordingly. Assume that Eve wants to spoof the identity of Alice.

She first listens to the communication between Alice and the BS, and then captures the IMSI of Alice. After a while, she sends a probe request to the BS. The BS will then request for the identity of Eve. Eve will then use the IMSI of Alice and will encrypt it using the private key of her eSIM and the public key of the SP, respectively. When the SP receives the plaintext IMSI and the encrypted IMSI, it will look for the public key that corresponds to the IMSI sent by Eve. After finding the public key, the SP will attempt to decrypt the encrypted IMSI. However, because the private key used to encrypt the IMSI does not correspond to the public key of the IMSI, the decryption fails, and the SP will find rubbish data. Subsequently, the SP detects the spoofing attempt, and the spoofing attack fails.

Chapter 6

Advantages

The advantage of using our scheme over some of the suggested schemes that are based on blockchain, machine learning, or quantum mechanics is that it uses less resources, and is much simpler, and it has been said that complexity is the enemy of security. Furthermore, our proposal can utilize well-known algorithms such as RSA and other public key cryptosystems that have proven their security for decades. Overall, the advantages of our proposal can be summarized as follows:

6.1 Simplicity

Our approach is based on a simple and well-known technology. Given that, the result schemes are simple and requires minimal effort for authentication. Given the simplicity of the scheme, it is much easier to verify its security when compared with other, more complex, schemes. Furthermore, public key cryptography is already a well-known science and is

a relatively easy concept to understand. This makes it more favorable as it doesn't require any additional knowledge, as opposite to quantum mechanics, for example. This in return will make its adoption easier and will contribute in its ease of implementation.

6.2 Ease of Implementation

Given the simplicity of our approach, it's not unreasonable to claim that it is easy to implement. Moreover, we can utilize well known public key cryptography cryptosystems such as RSA, which happens to be included in tens of libraries in many programming languages and tools. In contrast, other methods will require additional understanding and training, and potentially, outsourcing in order to be implemented.

6.3 No Third Party Required

A third party such as a CA is not needed in our approach as the UE is capable of verifying the authenticity of the BS by using the hardcoded keys. Which in return, contributes to the simplicity of our scheme. Furthermore, this has an added value of reducing the overall cost of deployment.

6.4 Cost Effective

Given that our approach is simple, easy to implement, and requires no third party, it can be reasonably claimed that it costs less, making it more cost effective. Further, unlike some of the suggested methods, our

approach does not require any specialized hardware such as those found in quantum communications, for example. Furthermore, given the simplicity of our approach, no additional training or outsourcing is required, which makes it less time consuming, and ultimately, cost effective.

6.5 Verified Security

The public key cryptography that is utilized in our approach has been the main driver for network security for decades. Which in return, verifies and proves its security, and ultimately, the robustness of our approach. In contrast, other suggested technologies such as blockchain, machine learning, and quantum mechanics are still in the experimental phase and have not been thoroughly tested.

Chapter 7

Conclusion

The future brings a new set of technical challenges that should be resolved. 5G QoS is no match for those challenges. 6G is expected to commercialize around 2030 to overcome such challenges. However, it is also important to plan the security at this phase.

Therefore, we proposed a different approach to harden the security of 6G by using public key cryptography and utilizing the eSIM to store the required cryptographic keys. The proposed scheme has few merits such as simplicity, ease of implementation, requires no third party, cost effective, and verified security. As future work, we will design a more optimized scheme utilizing the same principals and practically measure its performance against other schemes.

Bibliography

[1] Ali Al Mousa; Mohammad Al Qomri; Salman Al Hajri; Rachid Zagrouba (2020 IEEE) Utilizing the eSIM for Public Key Cryptography: a Network Security Solution for 6G (Pages: 1-6)

[2] Marco Giordani; Michele Polese; Marco Mezzavill; Sundeep Rangan; Michele Zorzi (2020 IEEE) Toward 6G Networks: Use Cases and Technologies (Pages: 55 - 60)

[3] https://www.gsma.com/esim/wp-content/uploads/2018/06/eSIM-Whitepaper-v4.11.pdf

[4] https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/connectivity/esim/what-is-an-esim

[5] https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/connectivity/esim/what-is-an-esim