NTNU – Trondheim
Norwegian University of
Science and Technology

Evolution of the SIM to eSIM

Elaheh Vahidian

Master of Telematics - Communication Networks and Networked Services (2
Submission date: Januar 2013
Supervisor: Van Thanh Do, ITEM

Norwegian University of Science and Technology
Department of Telematics

NTNU
Norwegian University of
Science and Technology

Evolution of the SIM to eSIM

Elaheh Vahidian

Master of Science in Communication Technology

Submission date: January 21, 2013

Supervisor: Van Thanh Do, ITEM

Norwegian University of Science and Technology

Department of Telematics

Problem Description

The SIM (Subscriber Identity Module) is security element used in the authentication of the subscriber before granting him/her access to the mobile network. The ingenuity of the SIM lies on the fact that it is a separate tamper resistant module which can be installed or removed from the mobile phone. However, with the advances in wireless and storage technologies there is proposal to replace the current SIM by the so-called soft SIM, which consists of a tamper resistant module soldered on the mobile phone and a software SIM downloadable over-the-air. This new SIM form factor could be even more flexible and convenient for the users but it could be challenging to ensure the same level of security. The goal of the project is to study and assess the security of the soft SIM. Another goal of the project is to investigate the business aspects of the soft SIM, which are fundamental to its success. The project will consist of the following tasks:

- Study of the different soft SIM solution propositions
- Security assessment of the soft SIM

Assignment given: 29 August 2012
Supervisor: Van Thanh Do, ITEM

Abstract

Every GSM (Global System for Mobile Communications) phone, also called 2G mobile phone and every UMTS (Universal Mobile Telecommunications System) phone, aka 3G mobile phone requires a smart card to connect and function in the mobile network. This smart card is called SIM, which stands for Subscriber Identity Module. In fact, this module contains the International Mobile Subscriber Identity (IMSI) and credentials that are necessary for the identification and authentication of the subscriber. Without the SIM the user will not be allowed to connect to the mobile network and hence not able to make or receive phone calls.

As a smart card the SIM is a tampered resistant microprocessor card with its own operating system, storage and built-in security features that prevent unauthorized individual to access, retrieve, copy or modify the subscriber IMSI and credentials. Abuses of subscriber's account and fraudulent accesses to the mobile network can hence be avoided. Furthermore, as a removable and autonomous module the SIM introduces great flexibility since the user can easily move the SIM to other mobile phones or replace a SIM with another one. So far, the smart card and its content, the SIM are bound together and called SIM.

With the advances in wireless and storage technology, new demands have arisen. Because of cumbersome task of opening machines and installing the removable SIM, the M2M applications are designed with pre-installed SIM application. The M2M applications based on the cellular networks with the ability of installing the user subscription have advantages and disadvantages for a certain stakeholder.

This master's thesis provides the multiple alternative solutions to this installation and also describe the SIM evolutions i.e. eUICC and soft SIM to give a comprehensive view of the SIM's situation. The thesis also presents the security assessment of these evolutions which are different with the current removable SIM.

Acknowledgment

Firstly, I would like to express my thanks to my supervisor Do van Thanh for his guidance and valuable advices. Last, but not least, I would like to express my heartfelt thanks to my beloved husband for his support and my beloved parents for their blessings and wishes.

Norway, January 2013
Elaheh Vahidian

Preface

This thesis is submitted to the Norwegian University of Science and Technology (NTNU) to fulfill the requirements for the Master of Technology degree. I would like to thank my supervisor Do van Thanh at Telenor for valuable help and support during my work with this thesis.

Trondheim, January 2013
Elaheh Vahidian

Abbreviations

2G	Second-Generation
3G	Third-Generation
3GPP	Third Generation Partnership Project
4G	Forth-Generation
A8	Algorithm 8, cipher key generator
AuC	Authentication Center
BS	Base Transceiver Station
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CHV	Card Holder Verification
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSIM	CDMA SIM
DoS	Denial of Service
EAL4	Evaluation Assurance Level 4
EAP	Extensible Authentication Protocol
EAP-RADIUS	Remote Authentication Dial In User Service
EAP-SIM	Extensible Authentication Protocol SIM
EEPROM	Electrically Erasable Programmable Read-Only Memory
EID	eUICC ID
EIR	Equipment Identity Register

EIS	eUICC Information Set
ETSI	European Telecommunications Standard Institute
eUICC	Embedded UICC
EUM	eUICC Manufactures
GGSN	GPRS Support Node
GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GSMA	GSM Association
GSN	GPRS Support Node
HLR	Home Location Register
ICC	Integrated Circuits Cards
ICCID	Integrated Circuit Card Identifier
IdP	Identity Provider
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
ISD-P	Issuer Security Domain Profile
LFSR	linear feedback shift register
ME	Mobile Equipment
MNO	Mobile Network Operator
MS	Mobile Station
MSC	Mobile Switching Center
NFC	Near Field Communication
NS	Network Subsystem
NSS	Network Switching Subsystem
OTA	Over-the-Air
PC	Personal Cmputer
PIN	Personal Identification Number
PLMN	public land mobile network
PUK	Personal Unblock Key
RAM	Random Access Memory
RAND	Random Number

RI	Right Issue
ROM	Read-Only Memory
RRC	Radio Resource Control
SC	Smart Card
SE	Secure Element
SIM	Subscriber Identity Module
SM	Subscription Manager
SM-DP	Subscription Manager Data Preparation
SMS	Short Message
SM-SR	Subscription Manager - Secure Routing
SSD	secondary security domains
SON-8	8-lead small outline non-leaded package
SP	Service Provider
SRES	Signed Response
SRID	Spatial Reference System Identifier
SSL	Transport Level Security
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TRAN	Transcoder and Rate Adaptation Unit
TRE	Trusted Environment
TSM	Trusted Service Manager
U	UserUniversal Asynchronous Receiver/Transmitter
UART	User Equipment
UE	Universal Integrated Circuit Card
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
WS-standard	Web Services Security standard
XRES	Authentication Response

Definitions

A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard.

CEIR, The Central Equipment Identity Register, is a database of the IMEI numbers of blacklisted handsets. If a device's IMEI number is listed on CEIR, it is not supposed to work on any service provider.

CSMG , a division of TMNG Global, is a leading strategy consultancy that focuses on the communications, digital media, and technology sectors.

ETSI, the European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT).

MVNO, a mobile virtual network operator, obtains bulk access to network services at wholesale rates into a business agreement with a mobile network operator and sets retail prices independently.

Trustchip, provides an end-to-end mobile protection - from the originating device, through the network, to the destination device. This can be visualized as a two-way secure tunnel that encrypts and mutually authenticates traffic regardless of vulnerabilities in underlying networks.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Mobile communications have become very essential part of our life. The technology creation, revolution and evolution of mobile wireless industry have been started since early 1970s and can be divided in the four generations of technology revolution and evolution. The first generation mobile system (1G) was analogue and only regional implemented such as AMPS (Advanced Mobile Phone Service) in the US and NMT (Nordic Mobile Telephone System) in the Nordic countries. Global System for Mobile Communications (GSM) is developed by the European Telecommunication Standards Institute (ETSI) represents the second generation (2G) mobile systems that are digital.

The Universal Mobile Telecommunications System (UMTS) is a third generation mobile cellular system which can co-exist with GSM and re-using multiple network elements while offering higher data rate. The long-term evolution (LTE), marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals.

Except the first generation, all the mobile systems require the presence of a SIM (Subscriber Identity Module inserted in the mobile phones before granting access to the mobile network and services. The SIM contains the International Mobile Subscriber Identity (IMSI) and credentials that are necessary for the identification and authentication of the subscriber. Without the SIM the user will not be allowed to connect to the mobile network and hence not able to make or receive phone calls.

As a smart card the SIM is a tampered resistant microprocessor card with its own operating system, storage and built-in security features that prevent unauthorized individual to access, retrieve, copy or modify the subscriber IMSI and credentials. Abuses of subscriber's account and fraudulent accesses to the mobile network can hence be avoided. Furthermore, as a removable and autonomous module the SIM introduces great flexibility since the user can easily move the SIM to other mobile phones or replace a SIM with another one. So far, the smart card and its content, the IMSI and credentials are bound together and called SIM.

Due to its ubiquity the mobile network is not only interesting in the provision of human communications, e.g. phone calls, SMS, etc. but also for other applications, especially M2M. M2M stands for Machine to Machine communications and refers to communications between devices. Typically, M2M uses a device (such as a sensor or meter) to capture an event (such as temperature, inventory level, etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information. Examples of M2M applications are logistics, fleet management, car safety, healthcare, and smart metering of electricity consumption.

To get access to the mobile network the device, i.e. meter, sensor, etc. has to host a SIM. Unfortunately, in most M2M usages, it is quite cumbersome, sometimes impossible to open the device and install the SIM card. Consequently, the SIM has to be installed at factory and preferably soldered on the printed board of the device. Such a factory installation is also required to make the SIM more robust and capable of resisting rough environments such as high temperature, pressure, humidity, noise, dust, etc.

The problem now is the fixed binding of the device with the mobile operator owning the SIM. Indeed, at manufacturing time it is usually unknown which country the devices will be shipped to and used. It is hence not possible to identify the mobile operator to order the SIMs. The only way to remedy the situation is to enable a way of posterior installation of the subscriber's IMSI and credentials. It is hence necessary to separate the smart card, now called UICC (Universal Integrated Circuit Card) and its content, which could be the SIM, USIM (UMTS SIM), ISIM (IMS SIM). Since the SIM is itself a software application on the UICC it is quite often denoted as "Soft-SIM", which can be downloaded via wire or over-the-air (OTA) to the UICC or eUICC (embedded or fixed soldered UICC). For wired downloading the eUICC can be empty since connections can be done directly to it. However, for OTA downloading the eUICC must contain a bootstrapping SIM which is sufficient to get access to the mobile network and to download the proper SIM.

The standardization work aiming at specifying the eUICC and the subscription management is still ongoing at ETSI and GSMA (GSM Association). The progress is quite slow due to the conflicting interests of the different stakeholders such as operators, SIM manufacturers, device manufacturer, service provider, etc. Currently, it is unclear what the consequences of the soft-SIM in terms of security will be. Therefore there is a need for a thorough security assessment.

1.2 Problem definition

Since extract, modify, or insert content in the SIM module in the removable SIM and tamper resistant devices are almost impossible for unauthorized user, hence the subscriber identity and credentials (e.g., secret key for the authentication) are very well protected and the fraud probability is very low.

With the original removable SIM the user's IMSI and credentials are very well protected and with the newer version of the authentication algorithms it is almost impossible to extract the secret key for authentication.

The emergence of M2M applications has created the need of separating the SIM application from the UICC and allowing over-the-air downloading of the SIM to the UICC. Although convenient for M2M applications this modification will surely bring new security threats that can be fatal but still unknown.

The main objective of this thesis is to shed light to the security challenges that the soft-SIM could introduces. More specifically, the main tasks of this thesis are:

1. Study of required background information
2. Study of different Soft-SIM solution
3. Study of possible authentication solutions
4. Security assessment of the Soft-SIM

1.3 Related work

Huge amount of research, documentation, and articles exist about the current removable SIM and their security solutions. In comparison the reprogrammable SIM is partially limited to research and documentation. Especially reading studies of security in the third evolution i.e. soft SIM, which only has been provided by Gehrmann.C [1]. This patent describes a very good survey of the method and apparatus which is soft SIM credentials securely transfer between devices. Schell.S et.al [2] also describe methods and apparatus for authenticating and granting a client device access to a network which is proposed by Apple.

There are some documents regarding to second evolution i.e. eUICC investigate by the GSMA (GSM Association) [3] [4] [5] [6] [7] which has developed requirement's documents for a reprogrammable SIM. The GSMA describes embedded mobile device requirements and use cases with the architecture of the remote provisioning system for embedded UICCs. The subscription management also is ongoing at ETSI and GSMA.

1.4 Methodology

This thesis gathers information of primarily refers to GSM and UMTS technologies that are commonly used in European Telecommunications Standard Institute (ETSI), and requirements and Use Cases described by GSMA. Also refer to understanding the most significant current SIM developments and the key technology and commercial issues with respect to the technology.

Because the design of the solution for the new technology of SIM so called Soft-SIM and their remote provisioning system must be driven by security concern in previous technology (e.g., embedded SIM), it is important to identify the whole architecture of the existing technologies in order to derive and meet the security requirements of today. Also provide recommendations and principles that will shape the final design.

The methodology used in this thesis work is both simple and logical. The work started with the study of background topics such as GSM, UMTS, smart card technology, UICC, SIM and security principles. Next, the different evolution paths of the SIM are thoroughly examined. Finally the security threats arisen from the changes of the SIM are assessed.

1.5 Organization of the thesis

The thesis is divided into five chapters. Table 1.1 presents a short description of each chapter.

Chapter	**Description**
Chapter 1 Introduction	The introduction contains a motivation for the thesis work, definition of the problem and a methodology of the thesis.
Chapter 2 Background Information	The background starts with an overview and introduction of the smartphone technology, GSM and UMTS architecture, traditional architecture of SIM and security peinciple of those technology.
Chapter 3 Evolution of SIM	This chapter starts with introduction of the SIM evolution and explains three paths of evolution. The chapter contains M2M SIM, eUICC provisioning process and ecosystem, subscription manager and GSMA M2M use cases. Finally the chapter is concluded with the Soft-SIM as a third evolution and market analysis.
Chapter 4 Security Assesment of the SIM	Security assessment of the SIM consists of security in M2M system, security requirements and security in Soft-SIM by considering of secure transferring in the Trusted Environment.
Chapter 5 Conclusion	The conclusion summarizes the thesis by considering to the evolution and security assessment.

Table 1.1: Organization of the thesis

Chapter 2

Background Information

2.1 Introduction to GSM

This chapter gives an overview of the basic functions and main entities in the GSM network with a short presentation of the GSM network architecture.

GSM (Global System for Mobile Communication) is a digital cellular technology used for transmitting voice and data services. GSM allows users to roam seamlessly from one network to another, while also providing personal mobility.

In 1989 the responsibility was passed onto the European Telecommunications Standard Institute (ETSI) for developing a standardized GSM system. GSM is a multiservice system, allowing communications of various types, depending on the nature of the transmitted information as perceived by the end users. GSM is the second generation of wireless communication systems, supporting both voice and data communications. In speech services, the information is voice, whereas in data services the information is such as text, image, and message and so on. In addition, both speech and signaling channels are digitalized, which essentially labeled GSM as the second-generation (2G) mobile system. It was developed in the mid 80's by the GSM consortium and it has grown rapidly since then. GSM provides a large palette of the services offered to fixed telecommunication users [8].

2.1.1 GSM Architecture

The GSM network [9] is composed of several functional entities which are divided into three main parts, with its entities and interfaces:

- Mobile Station (MS)
- Base Station Subsystem (BSS)
- Network Subsystem (NS)

The architecture of GSM is depicted in Figure 2.1 and the various entities are as follows:

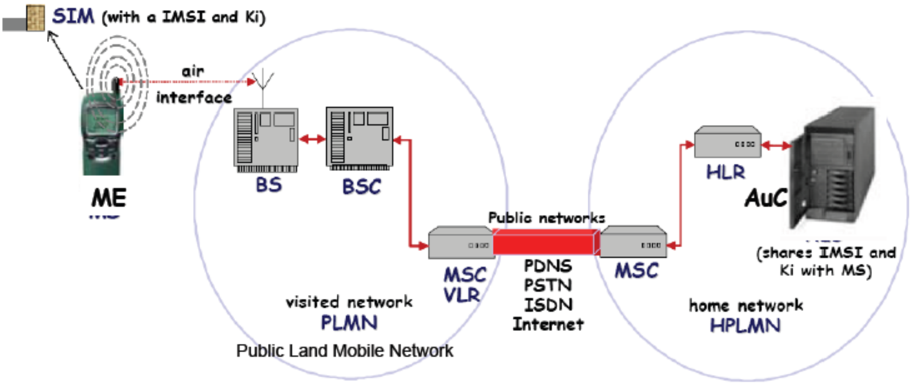

Figure 2.1: GSM Architecture [9]

Mobile Station (MS)

The MS is used by the subscriber as a communication device in the GSM network and consists of the physical Mobile Equipment (ME) and the Subscriber Identity Module (SIM). The SIM is independent of the ME, which means the SIM is a smartcard containing subscriber identity, authentication information and service information. It allows the subscriber to switch between different mobile equipment and still have access to the subscribed services. Without a valid SIM card, GSM service is not accessible. The SIM also contains secret subscriber key and other algorithms used for authentication and encryption. We will have a closer look at the MS security functions later on, since it is an important part of this assignment. The main purpose of the ME is to provide an interface to either a human user, via a microphone, loudspeaker, display and keyboard, or an interface to some other equipment such as a PC.

Base Station Subsystem (BSS)

The Base Station Subsystem (BSS) is the physical equipment controls all the radio related to a cell and needed to communicate with the MS's. The BSS is composed of the Base Transceiver Station (BTS) and the Base Station handover decisions, radio channels, paging coordination and other needed control functions. Figure 2.1 also is showing the BSS interfaces to the MS, NSS and GPRS Core Network. BTS transmits and receives signals to and from the MS. One or more BTSs are connected to the Base Station Controller (BSC) and these two make up the Base Station Subsystem (BSS). A base transceiver station is a piece of equipment that facilitates wireless communication between network and user equipment. The BSC provides the intelligence in a BSS. It controls a set of BTSs and manages them.

Network Subsystem (NS)

The NS controls multiple BSSs and manages the communications between two users and includes databases needed for additional subscriber, and mobility management. The central entity of the NS is the Mobile Switching Centre.

A single GSM network established and operated by a service provider is referred to as a Public Land Mobile Network (PLMN). In the following section, the key entities in a PLMN are briefly described.

Mobile Switching Centre (MSC)

The mobile switching center (MSC) is the primary service delivery node for GSM and is the core component of any NSS. This component controls several BSCs and is responsible for routing of incoming and outgoing calls. It also provides the management functions for terminal mobility such as registration, authentication, location updating, handovers and roaming.

Home Location Register (HLR)

The HLR is a database used for storage and management containing information of every subscriber that is authorized against the GSM network. The HLR stores subscriber information includes the International Mobile Subscriber Identity (IMSI), service subscription information, location information, service restrictions and supplementary services information. As a physical machine, an HLR is typically a standalone computer, without switching capabilities, and able to handle hundreds of thousands of subscribers [8]. There is logically one HLR per GSM network although it may be implemented as a distributed database.

Visitor Location Register (VLR)

The VLR is a database attached to one or several MSCs. When a subscriber roams away from its own network, information is forwarded from the subscriber's HLR to the VLR and it holds much of the same information as the HLR but in addition it temporarily stores subscriber data for those subscribers that are in the service area. A Temporary Mobile Subscriber Identity (TMSI) of the subscribers is also kept by the VLR. In most networks the MSC and the VLR are one and the same piece of equipment.

Authentication Center (AuC)

The Authentication Centre (AuC) is a function that provides authentication of each subscriber. The AuC holds a secure database storing identification and authentication key used for authorizing the subscriber access to the GSM network and responsible for generating authentication triplets of values consisting of a random number (RAND), a signed response $SRES$, and session key Kc. It is also a protected database that stores the secret subscriber key (Ki) from the subscriber's SIM card.

Equipment Identity Register (EIR)

The Central Equipment Identity Register is a database of the IMEI numbers of all cell phones reported stolen. The cell phone's IMEI number goes to CEIR[1], once a user reports to the operator about the theft. A common usage of the CEIR is with stolen cell phones. The EIR is a database contains the white, black, and the gray list. The white list contains all equipment identities that are permitted for communication. All equipment identities in the black list are denied. MEs appearing in the gray list are not necessarily denied, but are tracked for specific purposes.

Transcoder and Rate Adaptation Unit (TRAU)

The TRAU is responsible for compressing voice communication at the air interface. It is placed between the BTS and BSC or between the BSC and MSC.

Gateway Mobile Switching Center (GMSC)

[1] The Central Equipment Identity Register is a database of the IMEI numbers of blacklisted handsets. If a device's IMEI number is listed on CEIR, it is not supposed to work on any service provider.

The GMSC is an exchange between the PSTN and GSM network that recognizes mobile telephone numbers and is equipped with the capability to access the HLR for routing assistance.

International Mobile Subscriber Identity (IMSI)

The International Mobile Subscriber Identity (IMSI) is a unique number for every subscriber in the world. The IMSI is stored in the SIM card and also in the AuC. IMSI is not only a serial number identifying the MS but also display the manufacturer, type approval and the country of production, as described in the ITU E.212 [10]. It usually consists of 15 decimal digits. The three first digits are the country code, the next two or three digits are the network code. The remaining part of the number is the unique number within the specific network. When initializing the connection, only the IMSI is used. Otherwise to protect the subscriber a temporary identifier is used.

Temporary Mobile Subscriber Identity (TMSI)

The TMSI is stored in the VLR, which will keep track of all the subscribers residing in the area. Instead of IMSI, TMSI is used to prevent an eavesdropper from identifying the subscriber. A new TMSI is assigned for every location update involving a new MSC, the MS (SIM card).

Service Provider (SP)

The Service Provider initializes the authentication procedure and offers services to the users. It responds with an authentication request to the local supplicant on the mobile handset when receives a service request from a client, if the client is not already authenticated and if the security association is valid, the SP authorizes the client to the request service. Service Provider must be able to communicate securely with an Identity Provider to exchange authentication info.

Identity Provider (IdP)

The Identity Provider (IdP) is responsible for locating a suitable Authentication Server and it acts as an mediatory between the Service Provider, the Supplicant and the Authentication Server. The IdP translates EAP-RADIUS messages from the Authentication Server into EAP-SIM messages and passes it to the Supplicant.

Authentication Server

The Authentication Server is provided by the operator and is not our domain and is performing the actual user authentication against the GSM network.

2.2 The Universal Mobile Telecommunication System (UMTS)

The Universal Mobile Telecommunications System is one of the third generation mobile technologies. UMTS unlike the GSM (Global System for mobile communication) provides high data rates and low cost for data transmission and is secure against the known GSM attacks. GSM only supports subscriber authentication and encryption, whereas UMTS also provides integrity protection of the signaling traffic between the mobile station and a network. Figure 2.2, is shown the architecture of UMTS.

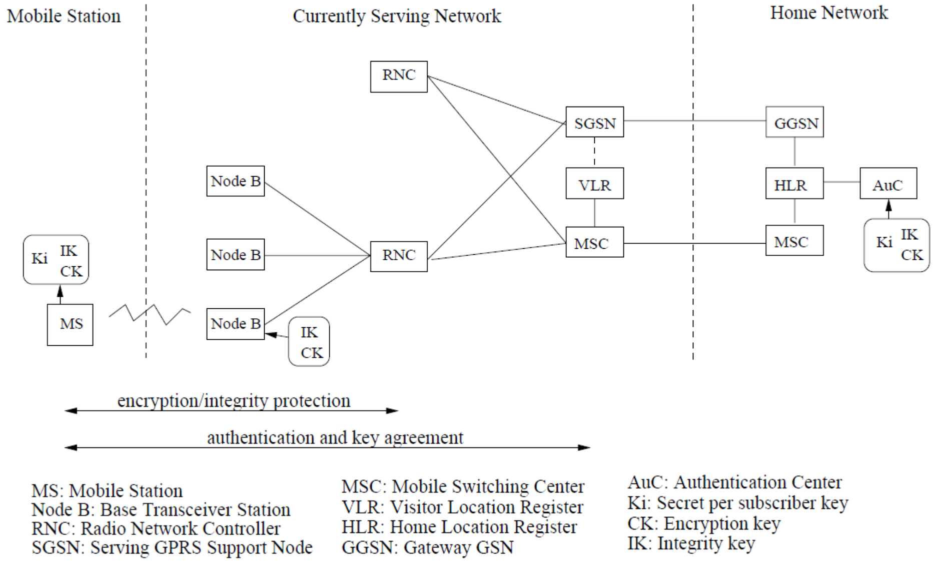
Mobile Station
Currently Serving Network
Home Network
RNC
SGSN
GGSN
Node B
VLR
HLR
AuC
Node B
RNC
MSC
MSC
Ki
IK
CK
MS
Node B
IK
CK
Ki
IK
CK
encryption/integrity protection
authentication and key agreement
MS: Mobile Station
Node B: Base Transceiver Station
RNC: Radio Network Controller
SGSN: Serving GPRS Support Node
MSC: Mobile Switching Center
VLR: Visitor Location Register
HLR: Home Location Register
GGSN: Gateway GSN
AuC: Authentication Center
Ki: Secret per subscriber key
CK: Encryption key
IK: Integrity key

Figure 2.2: UMTS Architecture and storage of secret key [11]

The radio interface is the mainly difference between the UMTS and GSM that applying other multiple access and channel coding techniques offering larger bandwidth per channel and more flexible channel coding [12]. The role of the RNC offers a combination of the functionalities of the BSC and the MSC, and is difference from the BTS in GSM. The HLR in GSM is called the Home Subscription Server (HSS), containing all subscription data including IP/telephone number, identities, service information and security support. GGSN id held the location information and the location updating takes place between the SGSN and GGSN. The RNC controls the radio resources. The mobile terminal in UMTS is called User Equipment (UE) and the base station are called node B.

2.3 The Smart Card technology

The successful story of GSM started in 1992 and within a few years it becomes the standard for mobile telecommunication systems. Better known of the Smart Cards (SC) that are used in GSM mobile phones is SIM. Smart Cards are mostly used as credit cards or SIMs. The SIM was and still is a pioneer when it comes to functionality and memory capacity among SCs. Regarding in both functionality and price, SCs can be subdivided into three groups [13]:

- Cards with surface contacts leading to a memory-only integrated circuit chip - memory cards;
- Cards with surface contacts leading to a microprocessor-integrated circuit chip -microprocessor cards;
- Cards with an electromagnetic connection to a microprocessor-integrated

Stored information, do not provide sufficient level of security and can be easily forged [14]. All later referrals to Smart Cards are microprocessor cards. Smart Cards are mostly used as credit cards or SIMs. Memory cards and microprocessor cards are two categories of Smart Cards or Integrated Circuits Cards (ICCs). Memory chip card acts as storage for information and provides almost no security gains compared to the magnetic stripe card [15].

An ICC (Integrated Circuit Card) or the name SC (Smart Card) is a portable, tamper-resistant computer containing a programmable data store. Technology of smart card is important for modern information. Since the deployment of smartcards is enormous because of the widespread usage of smartcards in international payment systems like MasterCard and Visa, ticketing systems and mobile phone networks by utilizing identification and access-control systems using security services by smart cards.

A SC operating system controls the interface for transferring data between the SC and a connected reader. Confidential data can be stored on the card in a secure way that prevents it from reading from outside due to the usage of cryptographic algorithms and security protocols. Data is stored, protected, and kept secret. The card body which holds the microcontroller, the chip hardware, the operating system and the applications are four components that are responsible for security of a SC.

The Third Generation Partnership Project (3GPP) was formed in the late 1990s to develop a more advanced and secure mobile technology system, which would eventually become the Universal Mobile Telecommunication System (UMTS). The SIM card evolved to become the Universal Integrated Circuit Card (UICC) smart card system under the 3GPP.within this system, components separated into UICC as a hardware and SIM as software.

2.4 Universal Integrated Circuit Card (UICC)

UICC stands for Universal Integrated Circuit card and is the smart card used in mobile terminals in GSM and UMTS networks. UICC is the best and only universal application delivery platform that works with any 3G or 4G device and ensures the integrity and security of all kinds of personal data. UICC contains a SIM application in a GSM network and a USIM application in a UMTS network. Thus, makes it possible for the same smart card to give access to both GSM and UMTS networks also provides storage of a phone book and other applications. The smaller size contains its own data storage and software than a full card.

In 2G networks the SIM card and SIM application were bound together, so that SIM card could mean the physical card, whereas in 3G networks, USIM, CSIM, and SIM are all three applications running on a UICC card. Thus, a card with the CDMA SIM (CSIM) [16], 3GPP USIM and SIM applications is called a removable user identity card (R-UIM) and works in all three cases. The other possible applications in the UICC called IP multimedia Services Identity Module (ISIM) that is required for services in the IMS [17], to secure mobile access to multimedia services, and non-telecom applications such as payment. IMSI is also stored within USIM application in the UICC.

One of the advantages is that the UICC can communicate using Internet Protocol (IP), the same standard that is used in the new generation of wireless networks. Also, it can support multiple PIN to protect personal information. A number of soft SIMs will be store in the UICC, not only for mobile phone communications but for future 4G and 5G communications.

2.5 Subscriber Identity Module (SIM)

A Subscriber Identity Module (SIM) is a removable smart card based on an embedded integrated circuit chip. The most important property from a security point of view is tamper-resistance. The Smart Card itself is called Universal IC Card (UICC) and SIM is an application running in the UICC. The SIM is a logical module that runs on an Integrated Circuit Card (ICC) type of Smart Card. Portability is the main property of smart cards, that in the case of a SIM, this property makes it possible for the GSM subscriber to move a SIM from one terminal device to another. It means a SIM card allows a user to change mobile devices by removing the SIM card from one mobile device and inserting it into another mobile device. However, another portability use case is that the subscriber replaces his normal SIM with a local pre-paid SIM in order to reduce roaming costs. A SIM card can have three identification data fields:

- The IMSI is the ID of the card that is used for identification with the network
- The MSISDN is the telephone number that is used to route incoming calls to the device
- The ICCID is the serial number for that SIM card

2.5.1 Traditional Architecture of SIM

SIM card is a smart card with a microprocessor and it consists of the following modules [18]:

- A Central Processing Unit (CPU)
- Working memory, Random Access Memory (RAM)
- Program memory, Read-Only Memory (ROM)
- Electrically Erasable Programmable Read-Only Memory (EEPROM)
- Serial communication module

The operating system is stored on the ROM and customized applications and data are typically stored on the EEPROM.

Current SIM architecture provides a more flexible environment in comparison of previous SIM design for handling application on the SIM. The new design of SIM, enable downloading of application via OTA (Over-the-Air) and enable interoperability across card manufactures for loading of Java-based applets onto the SIM card from any source. Figure 2.3 shows the current SIM architecture.

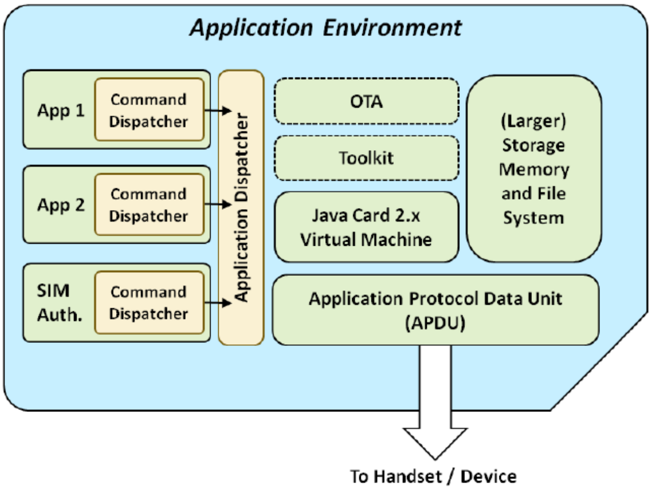

Figure 2.3: Current Java Card SIM Architecture [18]

The SIM card in the Java-based architecture runs a separate operating system from the device's operating system. The separation performs greater security for communication between the SIM and the device, and also allows the SIM card to act as a hardware firewall between the mobile device and the information on the SIM memory. The SIM/UICC Application Toolkit is a common elements shared by all applications which allows for manipulation of the application on the SIM. Figure 2.4, shows how other applications sit beside the SIM authentication applications in the Java-Card-based SIM architecture stack.

Device components such as OTA, USB and NFC allow interfacing with the SIM by protocols that are provided by the SIM architecture [18].

2.5.2 SIM Personalization Process

The SIM card vender will manufacture all requirements of MNO in the SIM cards and send back all the necessary data such as Ki, ICCID and OTA keys for the

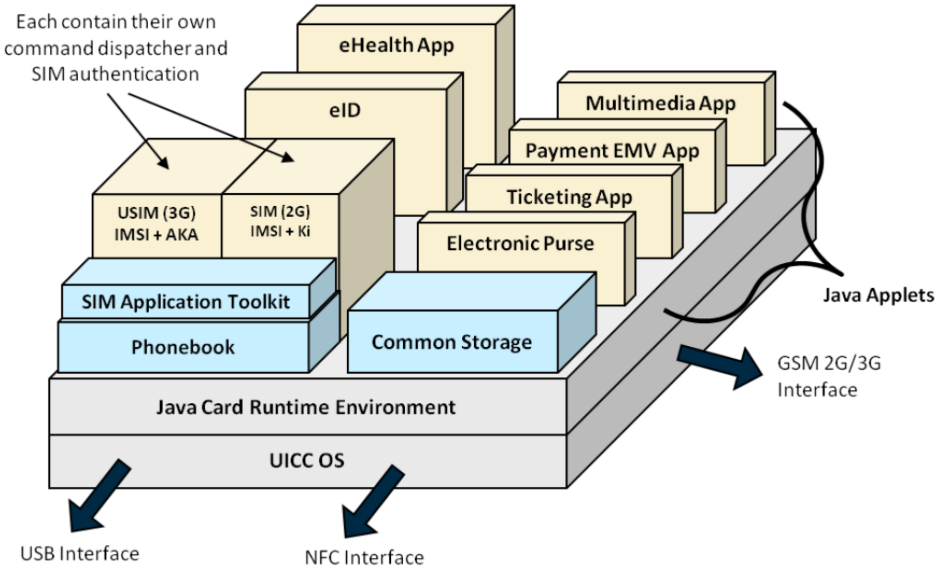

Figure 2.4: Java-Card based SIM Architecture [18]

operator to load into its own network system. There is a secure link between the SIM card vender and MNO to send information over secure link to ensure that critical data and key algorithms are not compromised. Each entity requires integration between the back-end servers.

The SIM card stores SIM subscription credential securely, and performs securely sensitive tasks. The SIM is used to store keys to authenticate mobile users, messages, and phone numbers and the subscriber credential, as well as the authentication algorithms A3/A8, and provides protected storage and protected execution functionality for security-sensitive data. The GSM application including the A3 algorithm is the one that we want to get in contact with. It will calculate a signed response and Kc by means of the A3 algorithm,and by challenging the GSM application with RAND [19].

Since a subscriber's identity stays with the SIM, a subscriber may move their phone number from one ME to another. GSM 11.11[20] describes the interface ME to SIM, and GSM 11.14 [21] describes the interface SIM to ME. The SIM and the Terminal can be produced by different manufacturers because the interface between the SIM and the terminal is standardized. For performing various calculations and reading data, there are several interfaces, but the SIM Supplicant only requires a subset of them. The specification of the SIM and the handset was considered part of the GSM standard.

The IMSI consist of 15 decimal digits. The first three digits indicate the home country of the user and the next two or three digits indicate a mobile network within that country, and the rest of digits identify the user within the network. The IMSI should be contained in the mobile terminal and the identity of the user was encoded in the mobile terminal, in earlier systems.

2.5.3 Roaming Architecture

The architecture of roaming is extensively similar to when at home, with the exception of protocols and standard processes. The visited network's VLR authenticates the subscriber identity of the device via the home network's HLR, without the Ki, IMSI or other sensitive information being revealed to the visited network. When the mobile device is turned on in the other network, the visited network confirms that it is not registered in its own database. Then, visited network attempts to identify its home network until finds roaming agreement between two networks, and maintains a TMSI for the device within its VLR. Likewise, its information will updates by home network to indicate that the mobile is on the host network. However, the all information that sent to the device can be correctly routed and any incoming calls can be routed to the correct BTS. Otherwise, when there is no roaming agreement between two networks, provision of service is not possible.

As shown in the Figure 2.5, authentication occurs in the visited network with the MSC and VLR of the home operator or the visited foreign network.

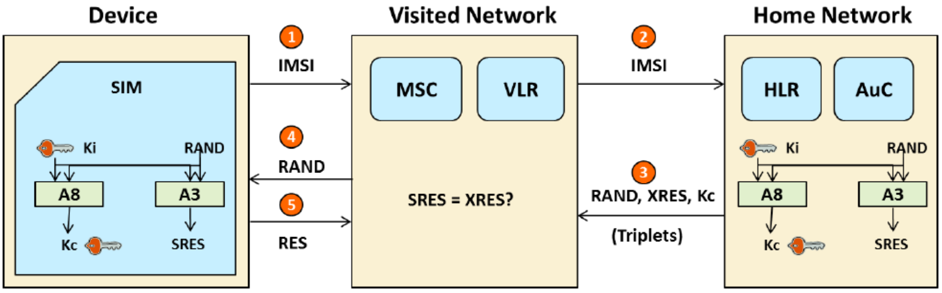

Figure 2.5: Roaming Authentication Process [18]

2.6 Security Principle

GSM was developed with focus in security. The goal of security design for the GSM system was that it had to be as good as wire line and it can be argued that GSM has even better security than wireline system. The user's main concerns are privacy and anonymity through strong user authentication, encryption and the use of temporary identifiers. The foundation of GSM security is the Subscriber Identity Module (SIM) that contains the subscriber identity (IMSI) and an associated 128 bits permanent key (Ki). One of the security goals was to make the system as secure as the PSTN.

2.6.1 GSM/UMTS Security

Security in GSM is divided in three main areas [22].

- Subscriber identity authentication
- Encryption at the radio interface for confidentiality of communication;
- Subscriber identity confidentiality

The security features of GSM are implemented in different parts of the GSM system:

- SIM Card
- Mobile Equipment
- GSM Network

At the transmission area, the use of air interface allows a number of potential threats from eavesdropping. Hence, the weakest part of the system was the radio path that can be easily intercepted. Every GSM network and all mobile equipment must support the GSM authentication scheme. But the operators have a free hand to implement their own algorithms within the GSM specifications. This is possible because the authentication is always going through the HLR, which is dealing with the computation of hashes and ciphers in some matter. However, the GSM security architecture is in such a way that can easily lock the broken card out of the system as soon as observing that tampering may have happened.

We will focus on the subscriber identity authentication service. This is the core of the GSM security system allowing seamless handover and roaming.

On GSM security there have been numerous attacks. Most of the effective attacks are based on physical access to the SIM. The GSM architecture will still be vulnerable against attacks on the operators' backbone network, regardless of broken security algorithms. It is well known that the security should be in the key and the algorithms in security systems should be open and tested by many independent security experts.

The SIM can be protected by different codes as PIN codes. PIN1 protects normal usage (like authentication) while PIN2 protects special services or blocks special numbers. Normally, the PINs will be blocked after a number of invalid attempts. PUK, the PIN Unlock is used to unlock the PIN. PUK1 and PUK2 respectively reset PIN1 and PIN2. If invalid PUK is entered a numerous times, the SIM will block local access to privileged information permanently.

The security mechanism in GSM is an example of how security can be implemented in a mobile system. The SIM authenticate and encrypt the information, and it defines which info contains in each entities. The authentication key Ki is a secret shared by the SIM card and the authentication center (AuC) that is a secure database only have access from HLR.

The AuC selects a random number R upon request from VLR and inputs this number together with the authentication key, and producing S in the algorithm A3. The key Ki and the random number R produce the encryption key Kc to use for encryption of messages by AuC using algorithm A8. The sets of R, S and Kc are sent to the VLR and the VLR don't need to request new authentication parameters every time the mobile terminal accesses the network and will simply reduce the signaling traffic between VLRs and HLRs.

In the GSM and UMTS the security issue is particularly important and the SIM contains the encryption key and the algorithm used for authentication the mobile user and the algorithm for computing the stream cipher key used for encryption. Since, the GSM security is intuitively simple, but cannot be said that the UMTS security mechanism is also same, where much more complex and less intuitive methods are applied. Since GSM base stations don't support integrity protection, an attacker can mount impersonation attack. However, the UMTS networks are secure against Man-in-the-Middle attacks, because the UMTS standard requires mutual authentication between the mobile station and the network depends on both the validity of the authentication and the integrity protection [11].

In UMTS network, a mobile station is connected to a visited network to a base station (Node B) and then is connected to a Radio Network Controller (RNC) that is controlled by a General Packet Radio Service (GPRS) Support Node (GSN). The Visitor Location Register (VLR) and the GSN keep track of all mobile stations that are connected to the network. In order to protect against attack, every subscriber is identified by its International Mobile Subscriber Identity (IMSI). The Home Location Register (HLR) keep track of the current location of subscriber of the home network that is dedicated to every subscriber which is shared a long term secret key Ki.

Mutual authentication accomplish between a mobile station and a visited network. The authentication and key agreement that is supported by both the network and the mobile station in UMTS is as follows (see Figure 2.6).

The base station and the mobile station establish a Radio resource Control connection (RRC connection), and the mobile station sends its security containing supported UMTS integrity and encryption algorithms to the base station. The mobile station also sends its current temporary identity TMSI to the network. If the network cannot resolve the TMSI, the mobile station answers the request with the IMSI.

Authentication data requested by the visited network from the home network of the mobile station, and then a random challenge RAND, the corresponding authentication token AUTN, authentication response XRES, integrity key IK and the encryption key CK will return by the home network. The visited network sends RAND and AUTN to the mobile station and AUTN verifies by the mobile station. The authentication response RES sends to the visited network and checks weather RES=XRES and decides to use security algorithms to sends to the radio subsystem. The radio access informs the mobile station of its command message which is integrity protected with the integrity key IK.

2.6.2 Identification

The process of identification, authentication and cipher key generation is described in Figure 2.7. Since the serving network does not have direct access to the per-

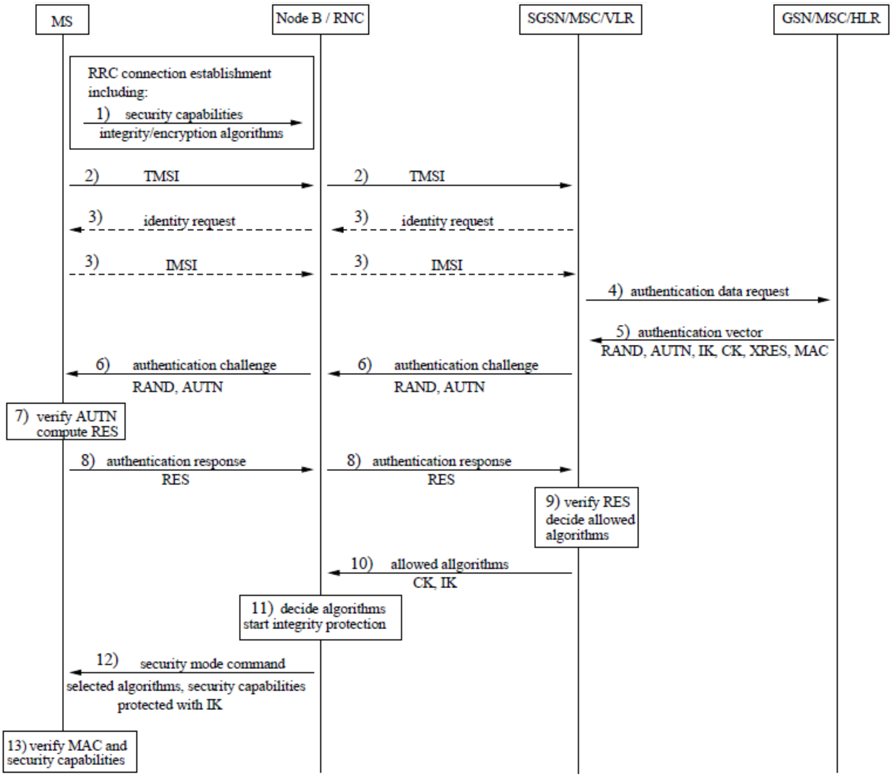
MS
Node B / RNC
SGSN/MSC/VLR
GSN/MSC/HLR
RRC connection establishment including:
1) security capabilities integrity/encryption algorithms
2) TMSI
2) TMSI
3) identity request
3) identity request
3) IMSI
3) IMSI
4) authentication data request
5) authentication vector RAND, AUTN, IK, CK, XRES, MAC
6) authentication challenge RAND, AUTN
6) authentication challenge RAND, AUTN
7) verify AUTN compute RES
8) authentication response RES
8) authentication response RES
9) verify RES decide allowed algorithms
10) allowed allgorithms CK, IK
11) decide algorithms start integrity protection
12) security mode command selected algorithms, security capabilities protected with IK
13) verify MAC and security capabilities

Figure 2.6: Authentication and Key Agreement in standard UMTS network [11]

manent key Ki, so it cannot perform the authentication alone. Hence, the authentication triplet RAND, SRES, and Kc are sent to the serving network element MSC/VLR from the AuC [22].

2.6.3 Authentication

Authentication levels are used to categorize different authentication schemes as shown in Figure 2.8. In terms of the consequences of authentication errors and misuse of credentials, four authentication levels are defined [23] where level 1 is the lowest and level 4 is the highest [9].

- Level 1 - Little or no confidence in the asserted identity's validity

- Level 2 - Some confidence in the asserted identity's validity

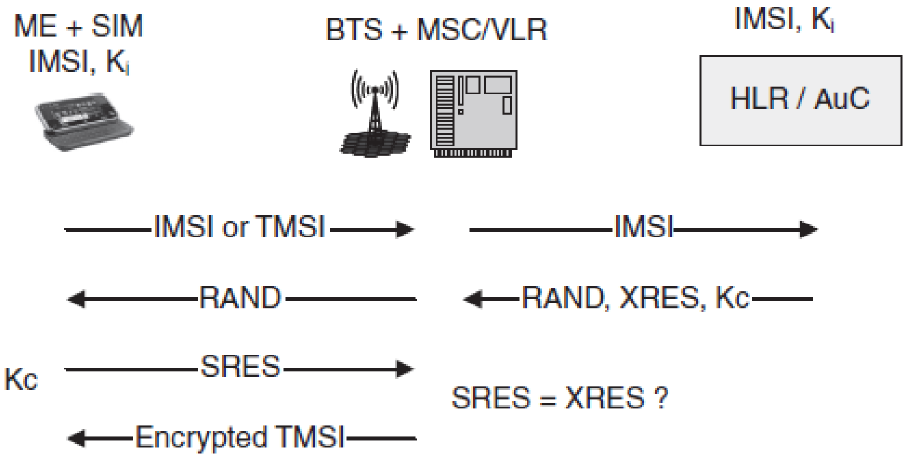

Figure 2.7: Identification and authentication of a subscriber [22]

- Level 3 - High confidence in the asserted identity's validity
- Level 4 - Very high confidence in the asserted identity's validity

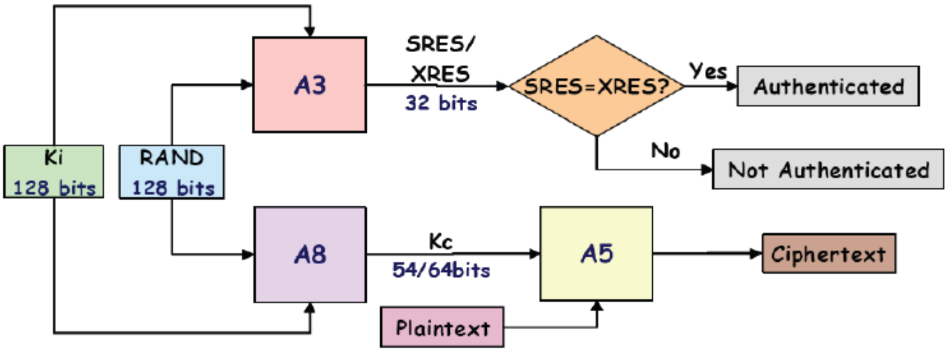

Figure 2.8: GSM Authentication, Cipher Key Generation and Encryption [9]

Authentication is very important in GSM since users are mobile and change their point of attachment to the network quite often. Authentication makes sure that only authorized users are allowed access to the network and that the bill goes to the right user. It also enables secure communication between the MS and the network by creating an encryption key, and it is one of the most important security functions in GSM. Authentication involves several functional components: the SIM card, MSC, VLR and the AuC. The SIM also contains some pre-installed keys and algorithms provided by the operator.

There are two different scenarios for the authentication of the subscriber that can land in. when the user is authenticated against the SIM, before the subscriber is allowed to use to use the GSM services, the SIM must authenticate against the GSM network. The first scenario is when the subscriber is located in a cell which belongs to a network never visited before. The second is when the subscriber is located either in its home network, or in a recent visited network.

The authentication scheme used in the GSM system is based on the A3 algorithm for authentication and the A8 algorithm for key generation. The A3 algorithm is a one-way function that generating the 32-bit Signed Response (SRES) required in the SIM authentication scheme. It should be easy to compute SRES from Ki and RAND, whereas the computation of Ki knowing RAND and SRES should be as complex as possible [24]. Subscriber Authentication Key (Ki), 128-bit, already stored in the SIM, along with a 128 -bit Random Challenge Number (RAND) generated by the HLR in the subscriber's home network. The A8 algorithm with the task of generating a temporary Cipher Key (Kc), is another one-way function [9]. (Figure 2.9)

Kc is used to encrypt phone calls on the radio interface, through the GSM symmetric cryptography algorithm A5. A5 is a stream cipher which is implemented very efficiently on hardware. The ME contains a cipher A5, used for enciphering/deciphering data against the MSC over the air interface. The input parameters in A8 are the same as input parameters in A3 and using the same mechanism as A3, to establish a cipher key Kc.

The Personal Identification number (PIN) or Card Holder Verification (CHV) is a 4 to 8 digit code used to authenticate the subscriber against the SIM card. The PIN is provided by the operator and is stored on the SIM card. If PIN is typed more than 3 times, the SIM card will be locked until an 8 digit Unblock CHV / Personal Unblock Key (PUK) is entered. The SIM will be permanently blocked when PUK is entered wrong 10 times. RAND, SRES and Kc are passed from the AuC to the VLR on demand and are only used once. The RAND must be 128 bits long and the SRES must be 32 bits long, since the Ki can be any format and

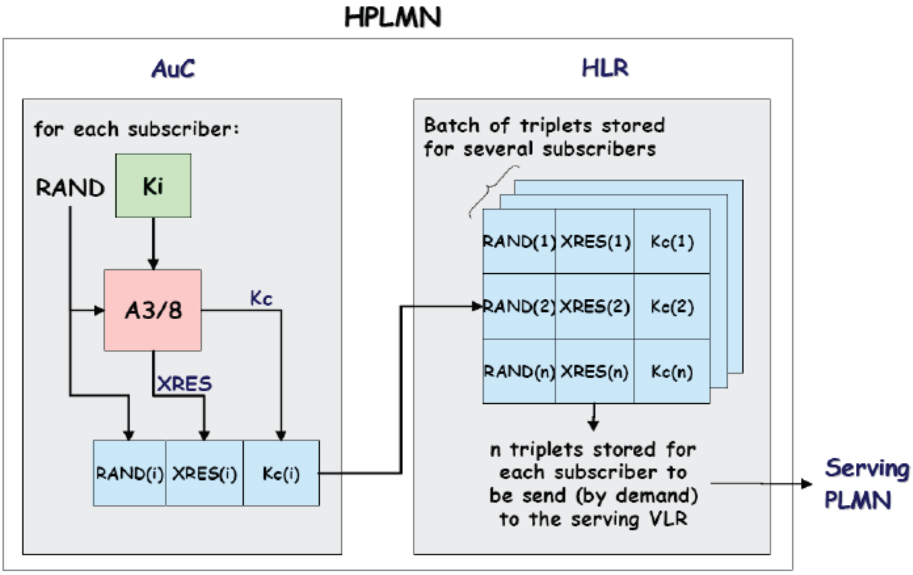

Figure 2.9: GSM Triplet Generation, Distribution and Subscriber Management [9]

length [9].

Visitor authentication is shown in Figure 2.10.

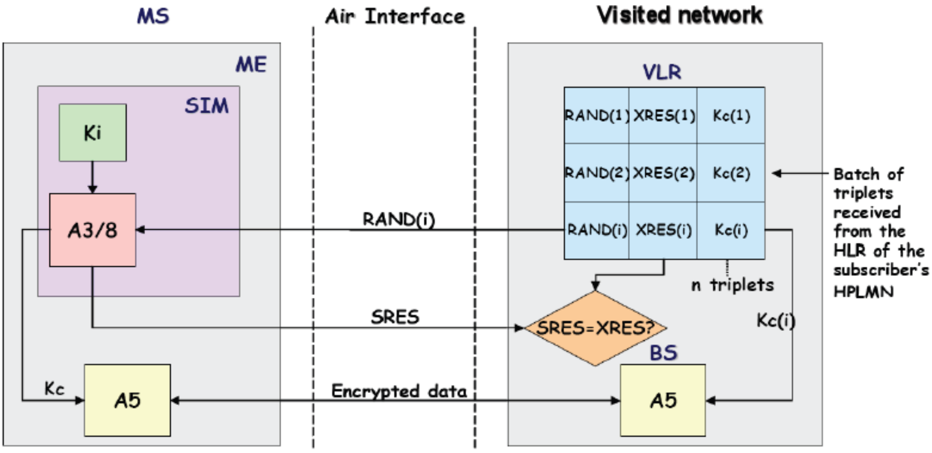

Figure 2.10: Authentication and Encryption for GSM using triplets and SIM [9]

2.6.4 Authorization

Authentication and Authorization are independent and before any Authorization, Authentication is necessary for clients in an un-trusted domain to allow verifying the identity of the parties without displaying shared secrets or keys. Authorization is the process of deciding if user X is allow to have access to service Y or not. To access a resource or make use of service, authorize the presenter of certain credentials.

For any future service request the user supply authorization token to access a resource or services. When services are requested for essential authorization, it should be protected from intruder and carefully constructed. Authorization tokens should be protected when making service request and should not be easily reproducible, and should prevent from reply attack.

2.6.5 Confidentiality

The purpose of subscriber Identity Confidentiality is avoiding an interceptor of the mobile traffic on the air interface. Confidentiality is the main security goal in GSM that is obtained by encryption of the link between the MS and BTS, and the encryption is based on the authentication. The SIM card also contains parameters needed to provide confidentiality, in addition of authentication.

A8 is an algorithm that is used to generate a session key Kc and Kc is used by a third algorithm called A5, a key stream of 228-bit from Kc. The stream decomposed into the two half that one of them encrypts the downlink frame and the other, encrypts the uplink frame [25]. The stream is calculated by A5 to encrypt and decrypt the frame. The A5 algorithm is implemented in the hardware not in the SIM card. The SIM runs the A8 algorithm to produce a 64-bit Kc by using RAND and the key Ki [9].

BTS starts encrypting when the command is acknowledge from ME. Figure 2.11 describes the GSM encryption algorithm is called A5 in its high-level structure. A5 generates consecutive sequences of 114 bits for encryption/decryption in the transmit/receive time slots. Encryption and decryption are performed by applying the 114 bits key-stream sequences to the contents of each frame using a bitwise XOR operation. A5 generates the key-stream as a function of the cipher key and the 'frame number', so the cipher is resynchronized for every frame. New Kc can

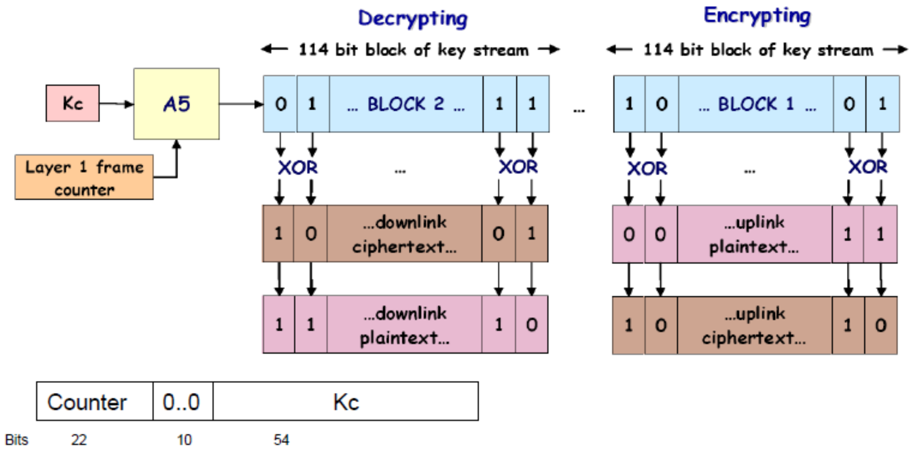
Decrypting
114 bit block of key stream
Encrypting
114 bit block of key stream
Kc
A5
Layer 1 frame counter
0 1 ... BLOCK 2 ... 1 1
1 0 ... BLOCK 1 ... 0 1
XOR
XOR
XOR
XOR
1 0 ...downlink ciphertext... 0 1
1 1 ...downlink plaintext... 1 0
0 0 ...uplink plaintext... 1 1
1 0 ...uplink ciphertext... 1 0
Counter
0..0
Kc
Bits
22
10
54

Figure 2.11: Operation of A5 at the mobile station [9]

be established to avoid key-stream repeat.

2.6.6 Denial of service

In the GSM system there is no mutual authentication but provides unilateral authentication. It means the MS is authenticated to the BS (Base Station), but the BS is not authenticated to the MS. So this property allows attacks one or more MS where a malicious third party masquerades as a BS.

In order to achieve the False BS attack, Figure 2.12 shows the steps in details [9]. Since the call between the False BS but within true SIM and the PLMN is an encrypted call, the PLMN does not see anything is going wrong. Whereas, the call from the target MS to the False BS is not encrypted and the link is eavesdropped at this point. So the BS attack can be detected later if the bill is checked.

Where an attacker makes the computing resource unavailable for its authorized users, a successful Denial of Service (DoS) attack performs. For example in the communication networks Node B, RNC or the bandwidth used for communication are the computing resources. This part introduces the Denial of Service attack in both GSM and UMTS network. As explained in the previous part, GSM technology provides unilateral authentication and is vulnerable to DoS attacks and the resources needed to mount such an attack are dangerously low. However, UMTS

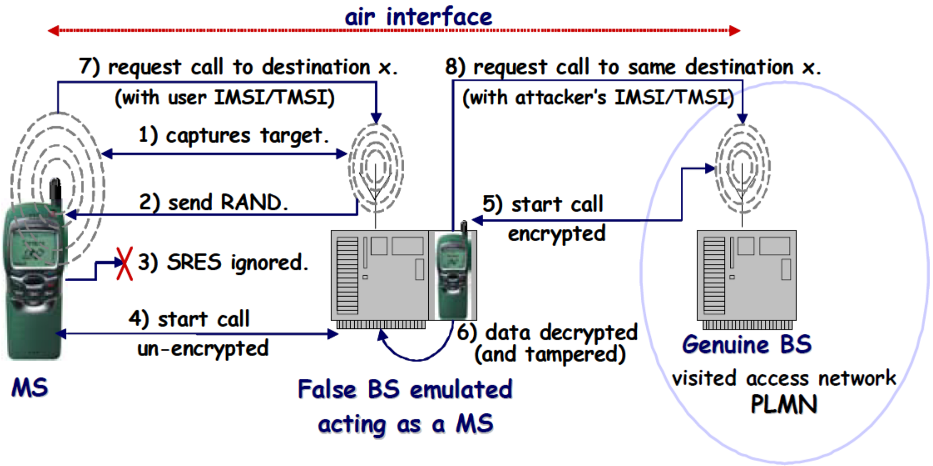

Figure 2.12: The False BS threat [9]

technology provides mutual authentication and is more secure than GSM, but still is vulnerable.

As is shown in the Figure 2.13, another kind of Denial of Service is for a false base station to capture a MS and prevent the MS communication. A False BS can impersonate a real PLMN to a MS indefinitely and is not necessary for the False BS to stop encryption on the air interface with Kc.

If the authenticity of the sender is hard to detect by the network, the user remains unreachable from the network and it detaches the legitimate UE to receive any calls. The other way described for the DoS attack is when the attacker sends a location update message from a different location instead of actual location. Therefore, the unreal location is registered in the network and any services will go for that user and location. Hence, the legitimate user does not receive any services and remains until it sends a location update message itself.

The International Mobile Subscriber Identity (IMSI) is very important for protecting user identity and is used only when it is absolutely necessary otherwise a Temporary Mobile Subscriber Identity (TMSI) is used. When user roam to new location, a new TMSI is assigned every time and is transmitted from the Serving GPRS Support Node (SGSN) to the UE with encryption and does not attach TMSI to IMSI until gets an acknowledgment from the UE. However, the SGSN does not know which TMSI is used and uses the IMSI to delete the old TMSI and starts a

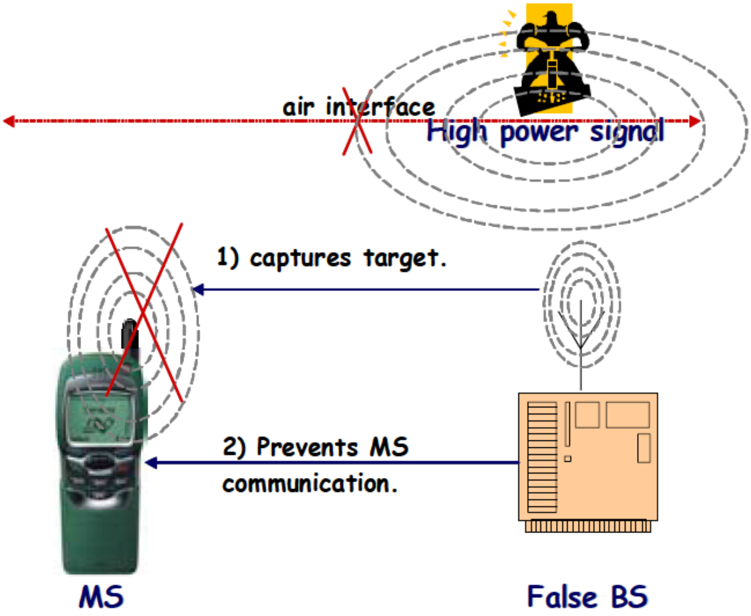

Figure 2.13: Denial of Service threats to GSM [9]

new TMSI. This attack can be sit in the handover zone and collect a large number of IMSIs by dropping the acknowledge message [26] (see Figure 2.14).

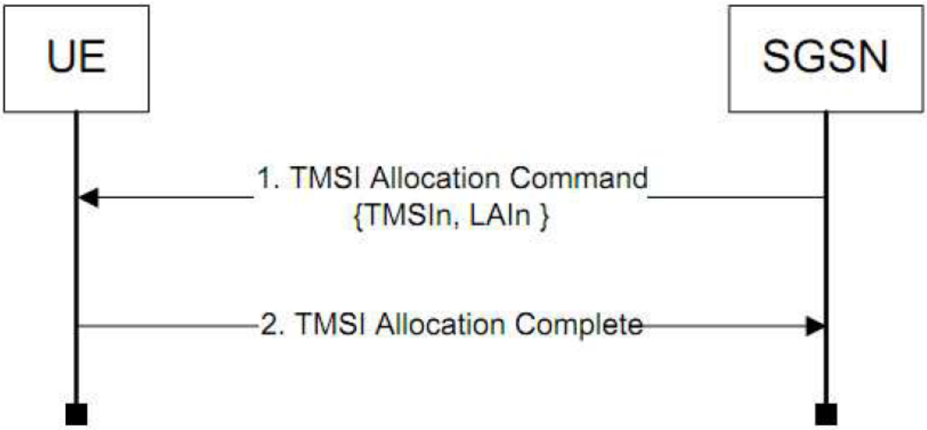
UE
SGSN
1. TMSI Allocation Command {TMSIn, LAIn }
2. TMSI Allocation Complete

Figure 2.14: TMSI allocation Procedure [26]

The next way of Denial of Service attack is when the attacker builds a database of collected IMSIs from the target network, then sends RRC connection request for each of the IMSIs in the database. The SGSN carries out all the tasks until the authentication. The attacker is unable to authenticate himself and is successfully overloading the network with heavy tasks and disallowing the legitimate users to authenticate themselves. In the 3G and UMTS technology, prevention of this attack is not carried out just by mutual authentication but also integrity protection of the start encryption command is required.

2.6.7 Non-reputation

Non-reputation is a service to provide proof of the integrity and origin of data, and also guarantees that the sender of the data cannot deny that the user sent it at a later point in time . So the easiest of these requirements to accomplish is proof of data integrity. However, an authentication with high assurance can be declared to be genuine and data integrity is best asserted. Since still is possible tamper with data through the threats. Non-repudiation of a mobile digital rights management (DRM) ensures that when a user (U) sends some message to a rights issue (RI), and user (U)/right issue (RI) can deny having participated in this transaction.

2.6.8 Privacy

GSM follows strict security procedures and will protect personal information where it processes or stores by privacy statements. Personal information collected by GSM is secured and are not available to the public. To provide Over-the-Air communication privacy use A5/1 (see Figure 2.15) that is a stream cipher in the GSM cellular telephone standard. Sequences of bursts are organized a GSM transmission and contain 114 bits available for information for each bursts. A5/1 produces 228 bits to XOR with the plaintext in each frame.

As shown in Figure 2.16, A5/1 is initialized using a 64 bits key with a 22 bits frame number. A5/1 [27] is a combination of three linear feedback shift register (LFSRs) with irregular clocking to produce pseudo random bit sequence, and consists of shift register-bit sequence and feedback function. The LFSR Period is the length of the output sequence before it starts repeating itself. The n-bit LFSR can be in 2n-1 internal states and the maximal period is also 2n-1. The tap sequence

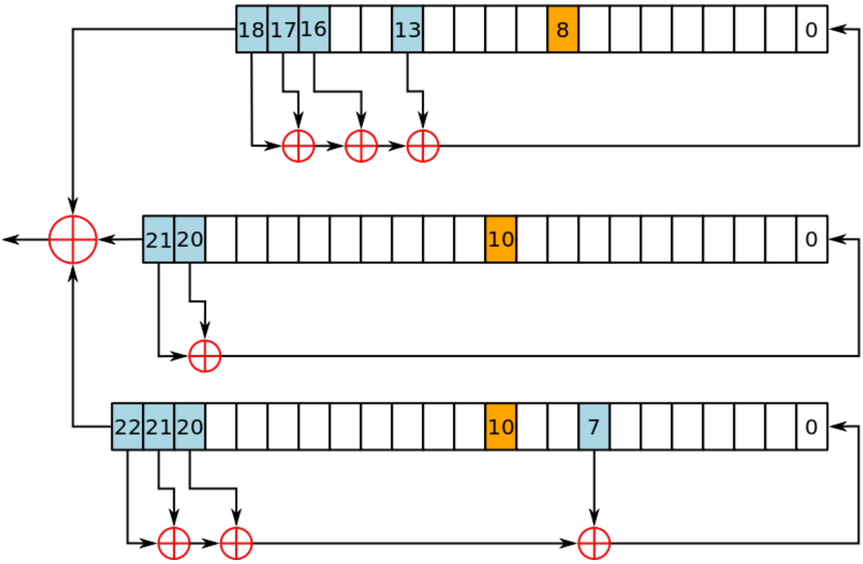

Figure 2.15: A5/1 stream cipher uses three LFSRs [27]

determines the period and the polynomial formed by a tap sequence plus 1 must be a primitive polynomial (mod 2).

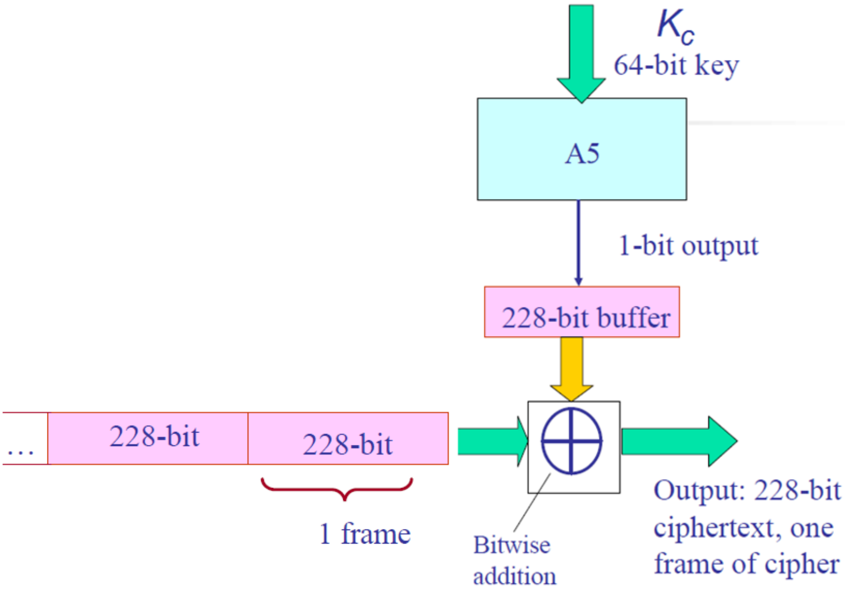

Figure 2.16: A5/1 and Frames [27]

Chapter 3

Evolution of SIM

3.1 Introduction

SIM cards have been made smaller over the years. As shown in the Table 3.1 [28], the evolution of SIM cards can be broken down into five period of time. Full-size SIMs were followed by mini-SIMs, micro-SIMs, and nano-SIMs. SIMs are also made to be embedded in devices. However, the current SIM cards that are used worldwide are changes from Full size to Mini SIM. Mini SIM cards have the same thickness as full-size, but their length and width are reduced. SIMs for M2M applications are available in a surface mount SON-8 package which may be soldered directly onto a circuit board [28]. Nano-SIM card which were designed in conjunction with Apple by the European Telecommunication Standard Institute (ETSI), are 60% physically smaller than the existing SIM cards.

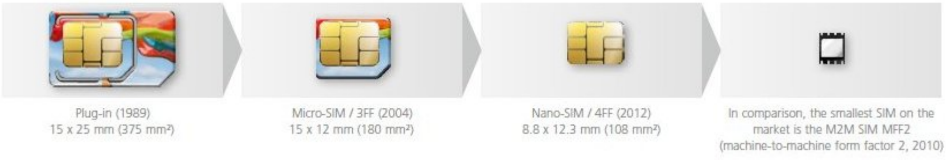

Figure 3.1: SIM from factors in comparison [29]

Figure 3.1 shows the evolution of SIM cards and the next generation of SIM

Table 3.1: SIM card sizes

SIM card	Standard References	Length(mm)	width(mm)	Thickness(mm)
Full-Size	ISO/IEC 7810:2003,ID-1	85.60	53.98	0.76
Mini-SIM	ISO/IEC 7810:2003,ID-000	25.00	15.00	0.76
Micro-SIM	ETSI TS 102 221 V9.0.0.Mini-UICC	15.00	12.00	0.76
Nano-SIM	EtSI TS 102 221 V11.0.0	12.30	8.80	0.67
Embedded-SIM	JEDEC Design Guide4.8,SON-8	6.00	5.00	¡1.0

cards, ’nano-SIM’. (Full-size SIM (1FF), mini-SIM (2FF), micro-SIM (3FF) and Nano-SIM (4FF))

However in the context of this thesis the focus is not on the form factor of the SIM but on the management of the SIM. The SIM evolution in terms of management is still unclear and unsure due to a lot of political and economic factors. To give a comprehensive view of the situation a simplified description of the evolution is given in Figure 3.2.

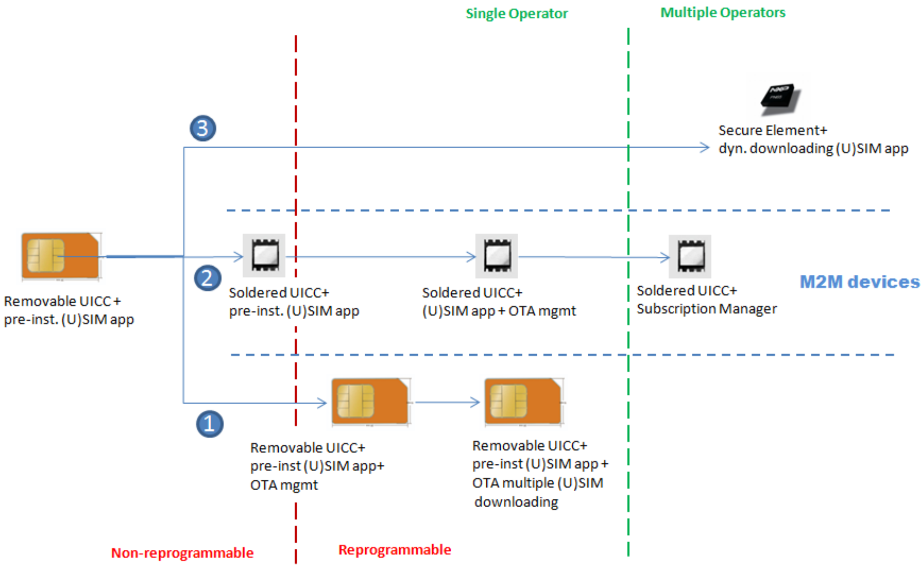

Figure 3.2: The SIM evolution

As shown in Figure 3.2 from the current removable SIM, which is a UICC with a pre-installed SIM or USIM application there are three evolution paths:

- Evolution Path 1: Removable UICC
- Evolution Path 2: M2M SIM
- Evolution Path 3: Soft SIM

All the three evolution paths will be successively explained in the following sections.

3.2 Evolution Path 1: the removable SIM

In this path the SIM will remain the same as today, i.e. consisting of a UICC hosting a SIM or/and USIM belonging to one operator. However, there will be Over-The-Air (OTA) management facilities allowing the dynamic modification of the user subscription and settings remotely over the mobile network. The UICC can also store multiple subscription profiles, i.e. job and private that could be selected and used by the user.

3.3 Evolution Path 2: the M2M SIM

3.3.1 Embedded Module Architecture

Mobile network are starting to be used to connect all sorts of devices. The traditional removable SIM may not be appropriate for certain applications. Therefore, SIMs may be embedded in devices at manufacture that may even be in advance for choice of country of use and for coice of network operator. During life time of the device, network operator may be changed.

The Embedded module will be housed in the devices such as a car, vending machine or medical device. Some Embedded Module devices may be not enable embedded applications to run in an application execution environment and may be used only as a modem. The other embedded module may run on a processor embedded in the based band itself, or run on a separates standalone processor with enough resources [6]. Figure 3.3 shows the architecture of the Embedded Module.

Depending on application, the use of hardware interfaces is required or optional on Embedded Module. For example in Mini-card the supported interfaces i.e. power, antenna, 12C, Inter-Integrated Circuit UART and UICC are required.

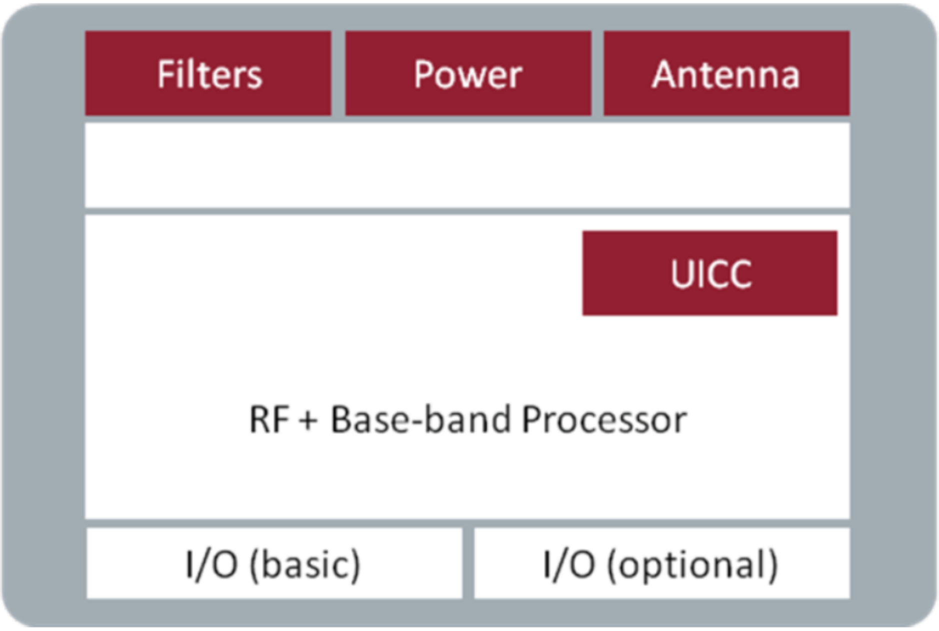

Figure 3.3: Embedded Module Architecture [6]

All modules need to be supported a basic set of services and also optional services at specific applications. The opportunity of employing these services will be managed by restriction of bandwidth, processing capability and memory capacity.

The following include the Basic Set of Services:

- SMS
- Packet Switch Data
- IP
- TCP
- UDP
- ICMP

Following also include optional services at specific applications. Some of them may be necessary in specific Use Cases:

- Emergency Call
- MMS
- Email
- Circuit Switched Voice
- Circuit Switched data
- Video call
- Location Based services
- MultiCall
- Group 3 Fax

For example in some Embedded Module applications require to automatically generate outgoing e-mail messages. So if this optional service is required, the necessary Internet Protocols must be implemented in the Embedded Module or on the Host Device.

Because of difficulties and cost associated with the physical access to the Embedded Modules and Embedded Devices, UICC need to be remotely managed. When the connectivity of Embedded Module devices and the network is turned off, and the Embedded Module device signaling capability is stopped altogether, this would introduce a significant new denial-of-service security risk. Hence, turning of the embedded device and the network is not recommended. However, some limitations are imposed on the frequency of signaling either via Embedded Module device or network-based modifications.

The embedded UICC (eUICC), a reprogrammable SIM which has defined by GSMA [3] as a small trusted hardware component that may be soldered into mobile devices to run the SIM application. The eUICC also enables the secure changing of other subscription data and identity, and performs the role of a traditional UICC. The eUICC is not intended to be removed or replaced in the terminal, but also it is soldered into mobile devices to run the secure network access applications and securely changing subscription data and identity.

Embedded UICC is a combination of things. It is a traditional UICC with additional features and an ecosystem. Embedded UICC is an UICC that supports remote management of operator credentials, and it is supporting set of interfaces and standards that allow operator credentials to be transported securely from the Operator to the UICC. It is also an ecosystem that provides the integrity and trust necessary to protect Users and Operators during the transport and provisioning of sensitive data and industrial secrets. The eUICC also is a proposal for an ecosystem to ensure secure and trusted operation and consists of a modified UICC card and necessary interfaces and processes. Since, it is not removable; there is a need to be reprogrammable.

The origins of embedded UICC is current UICC which is getting smaller in size over time in such as Machine-to-Machine (M2M) devices, and the UICC is soldered directly onto the circuit board. The architecture must support a level of security that we have in the current level of security. All entities involved in the management, for platform and profile management have to be mutually authenticated. The devices manufacture for M2M vendors with ”blank” SIMs can provision in any country. The eUICC has key benefits in the M2M where SIMs may be non-removable. M2M customers have also benefits of changing their connectivity service provider regardless of number of devices.

Typically, M2M uses a device to get access to the mobile network and is sometimes impossible to open the device and install the SIM card. In many M2M device categories the SIM has to be installed at manufacture using non-removable SIMs and preferably soldered on the printed board of the device with the ability of downloading SIM or USIM Over-the-Air management. Hence, the device, i.e. meter, sensor, etc. has to host a SIM. In utility industry M2M technology can help improve energy efficiency by remotely monitoring equipment, reading meter and tracking usage. Also in transportation M2M communication works with GPS and GSM technology to track vehicles and improves functionality and safety through fleet management services such as remote diagnoses.

The following are supported by the Embedded SIM or eUICC ecosystem [4]:

- The ability of remote management of operator credential in an Embedded

SIM

- Embedded SIM is a set of interfaces that allow operator to transmit securely to the UICC
- Provisioning of sensitive data and provide the integrity and trust necessary to protect users and operators within the ecosystem.

Embedded SIM will have a potential to support the five major business use cases listed which is explained in the GSMA Use Cases in details. M2M Service Providers need multiple provisioning and need an ability to change subscriptions. Consumers also need flexibility to support many different distribution models and if SIMs can never be removed from a device, safety nets need to be presented at the end of life or when devices fall in the wrong hands.

Following Use Cases are required to support M2M service provider:

- **Provisioning of multiple M2M subscriptions:** An M2M Service Provider sets-up subscriptions for a number of connected M2M devices to start telecommunication services with a Network Operator.
- **Provision of first subscription with a new connected device:** A subscriber purchases a new type of connected device from a device vendor / distribution channel.
- **Subscription Change:** A subscriber changes the subscription for a device to stop services with the current MNO and start services with a new MNO.
- **Stop Subscription:** A subscriber sells his device and stops the subscription for services from the current MNO.
- **Transfer Subscription:** Subscriber transfers subscription between devices.

3.3.2 eUICC single-profile and multi-profile swapping

Where the SIM is embedded in the eUICC model, the consumer may have to ask the Subscription Manager (SM) to do the switch, whereas in a traditional removable SIM model the consumer can change SIMs by physically removing a SIM and replacing it with another. If a Subscription Manager does not link to all

MNOs, the consumer may unable to switch to a particular operator. In this case, for preventing of fragmentation risk in this new ecosystem, a degree of industry cooperation and standardization that is being considered by ETSI[1]are required. ETSI and commercial deployments currently are being created M2M standards for eUICC, so the main focus of this technology has been M2M.

Their functionality could be increased by enabling swapping rather than just switching. As explained in the last part, switching is defined if consumer replaces their SIM profile permanently with new MNO and don't expect to use the previous one anymore, whereas in SIM swapping the SIM profiles replace temporarily. Swapping can be done either nationally or internationally. In the nationally part, the consumer swaps profiles to connect to different operators within the same country that bring coverage and consumer gets benefits of cost and quality of service. However, in the internationally part, consumer connects to a particular network when is going abroad but retain home subscription profile for return.

When using eUICC, consumer would select and download local subscription Over-the-Air without having physically obtains a new SIM in swapping. Two models of swapping consist of: "single profile" and "multi profile".

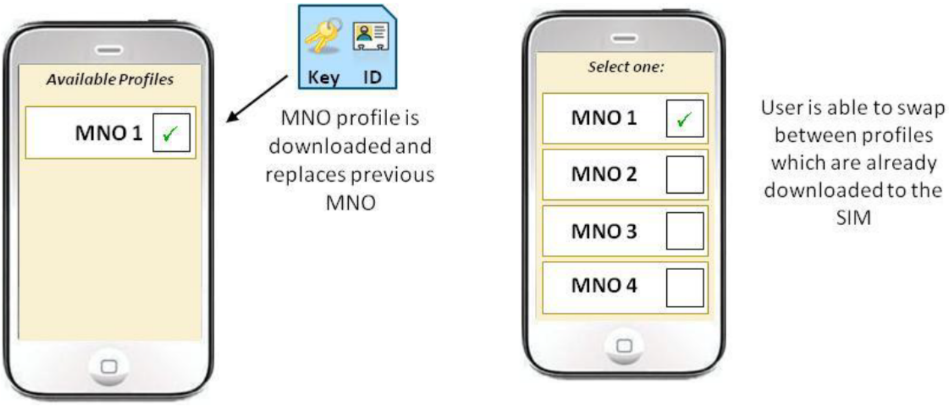
Available Profiles
MNO 1 ✓
Key ID
MNO profile is downloaded and replaces previous MNO
Select one:
MNO 1 ✓
MNO 2 □
MNO 3 □
MNO 4 □
User is able to swap between profiles which are already downloaded to the SIM

Figure 3.4: Comparison of eUICC single-profile and multi-profile swapping [18]

In the single profile, a new profile is provisioned each time user swaps mobile operator and the old profile is overwritten or deactivated as the SIM can only hold

[1] The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT)

the active MNO profile at a time. So it has a disadvantage when the consumer would like to swap back to their original profile. Hence, MNO would need to store profiles for subscribers. However, in a multi profile system more than one profile can be stored on the SIM. In this case both old and new profiles stay active on the MNOs' system and the user allows swapping between profiles without needing to repeatedly download profile from the MNO.

In this way, Multi-IMSI SIMs also as shown in the Figure 3.4 are currently able to swap between multiple different MNOs. Swapping model could also bring coverage, cost and quality of service benefit to consumers. For example, consumers could swap network or tariffs depending on the offer and they might also switch networks to improve quality on their current network.

Multi-profile solution in the nationally swapping requires a number of pre-installed profiles on a device to activate their preferred option to provide intelligent cost and coverage management.

In the marketing view, swapping is not beneficial for MNOs and commercial perspective but can provide a number of benefits to consumer with regard to choice, convenience, cost and mobile coverage. However, there is also some harm or restriction for consumer such as switching that may exacerbate in embedded SIMs rather than removable SIMs.

Likewise because of existing more IMSIs in the Multiple IMSI solutions, requiring advance planning to pick and to use the correct Multi IMSI before going abroad. Current international roaming solutions provide a convenient connection for users but with higher "roaming rates", whereas with the eUICC, the consumer has ability to download a "local profile" Over-the-Air and switch to a local connection and take advantage of local tariffs.

For allowing the consumer to switch to a local connection, there is a need to understand a multi-IMSI and its solution. A Managed Service Provider (MSP) forms several Mobile virtual network operator MVNO [30] relationships in different countries and produces a SIM that contains multiple IMSIs. The SIM automatically can change to the correct IMSI when it detects a new country. The calls will receive on both number and all charges will receive on a single bill for the consumer [18].

To switch between multiple profiles on a SIM, eUICCs utilize multi-IMSI technology such as a provisioning profile between two operational MNO profiles or between a MNO profiles. Multi-IMSI SIM contains two or more IMSIs on a single

SIM. Each IMSI has its own Ki that generally provided by travel SIM providers. Since the IMSI and Ki are preloaded Over-the-Air on the device rather than written to the SIM card, so current Multi-IMSI SIMs are not reprogrammable SIMs.

3.3.3 eUICC Provisioning Process and Ecosystem

Embedded UICCs in the Embedded Mobile Devices compare with UICCs may not allow subscriptions to be easily changed via physical access to the UICC, so they need to solve this problem by Over-the-Air remote provisioning of Embedded Mobile Devices. The same level of security and authentication protocols will be used.

The procedures describes in this section involve interaction between a customer and service provider in the business environment, between eUICC and SM-SR and also interaction of SM-DP and SM-SR in the remote provisioning architecture.

When an eUICC is manufactured, the master keys that are issued by the eUICC will load to SM-SR database and allow the SM-SR to access the eUICC and download new operator profiles to the eUICC. The SM-SR become connects with a SM-DPs that are packaged by the MNO SIM credential, including the IMSI and Ki, for secure download between the SM-SR and a new eUICC. This secure communication occurs over a ”provisioning profile” or ”setup bearer” [18]. Figure 3.5 shows the provisioning ecosystem of eUICC.

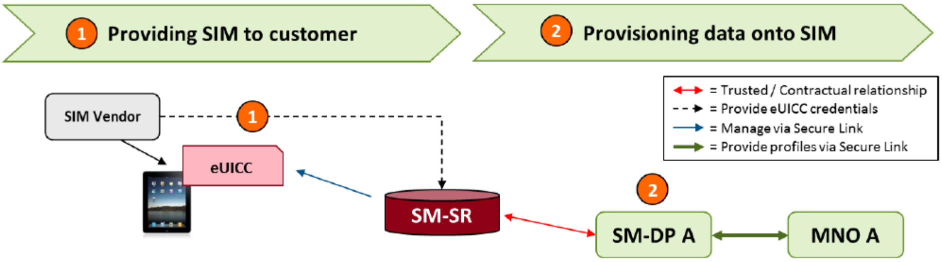
1 Providing SIM to customer
2 Provisioning data onto SIM
SIM Vendor
1
eUICC
SM-SR
= Trusted / Contractual relationship
= Provide eUICC credentials
= Manage via Secure Link
= Provide profiles via Secure Link
2
SM-DP A
MNO A

Figure 3.5: eUICC Provisioning Ecosystem [18]

The procedures of eUICC Provisioning Ecosystem describe in details in this part. The main steps for each procedure are ”Start condition” and ”End conditions”.

3.3.3.1 eUICC Registration at SM-SR

The eUICC manufactures (EUM) registers the eUICC at a selected SM-SR, otherwise remote access to the eUICC will be impossible.

Start Condition: In the Start condition eUICC are produced and has a corresponding Information Set (EIS). Provisioning profiles is loaded and active in the provisioning operator's network and are ready to ship.

Procedure: As shown in the Figure 3.6, the eUICC manufacturer (EUM) sends a eUICC registration request containing eUICC information Set (EIS) to the selected SM-SR. Then, EIS with the eUICC-ID (EID) as the key parameter stores in the SM-SR. To the EUM, the successful registration confirm by SM-SR including the EID message.

End condition: The eUICC now is registered at the SM-SR and is ready to download profile and ship to the device manufacturer.

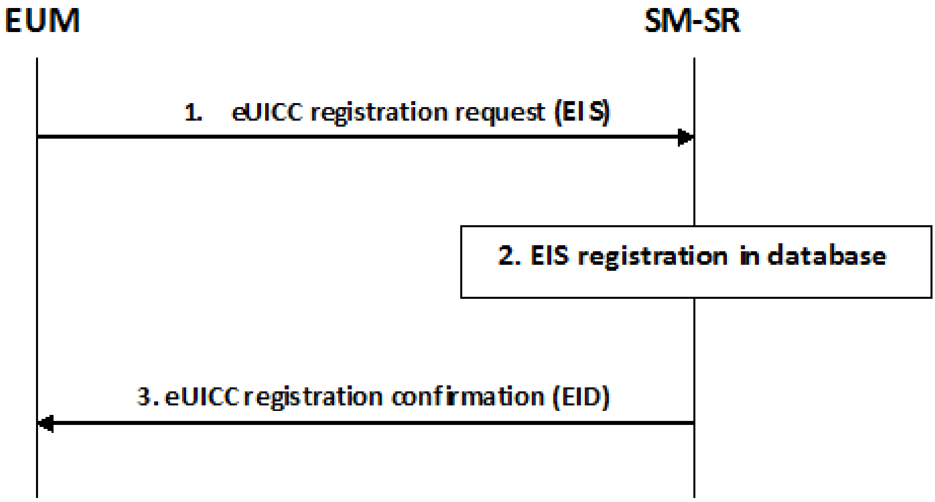
EUM
SM-SR
1. eUICC registration request (EI S)
2. EIS registration in database
3. eUICC registration confirmation (EID)

Figure 3.6: eUICC Registration at SM-SR [5]

The communication between EUM and SM-SR are secure and each eUICC may be registered at one SM-SR.

3.3.3.2 Profile Ordering

MNO order profiles under their responsibility within the eUICC. The procedure is the same as the current UICC but the only difference is that the eUICCs are not produced in physical form but are kept at the SM-DP as profiles.

Start Condition: between the MNO and the SM-DP profiles are defined in a separate process.

Procedure: As Figure 3.7 shows, the MNO provides an order contains the MNO profile specification, an IMSI or a list of IMSI to a selected SM-DP. During the personalization process by the SM-DP, keys or ICCID may be generated. Register the Profiles and confirm order completion by MNO and installs the Profiles in the related systems for example HLR, AuC and CRM.

End Condition: The Profile download procedure is ready.

3.3.3.3 Profile Download and Installation

For the communication services of the devices, the eUICC with at least one operational Profile Over-the-Air must be loaded. The Profile download and installation procedure is shown in the Figure 3.8.

Start Condition: a customer has subscribed to a selected MNO. Meanwhile, the MNO knows the EID of the target eUICC and the SRID. A Profile ordering procedure has been completed with a selected SM-DP and the target eUICC is associated to an SM-SR. the related subscription in the network may activate by the MNO.

Procedure: The request of Profile Download that is included the relevant information sends to the SM-DP by the MNO. The MNO also once the Profile is

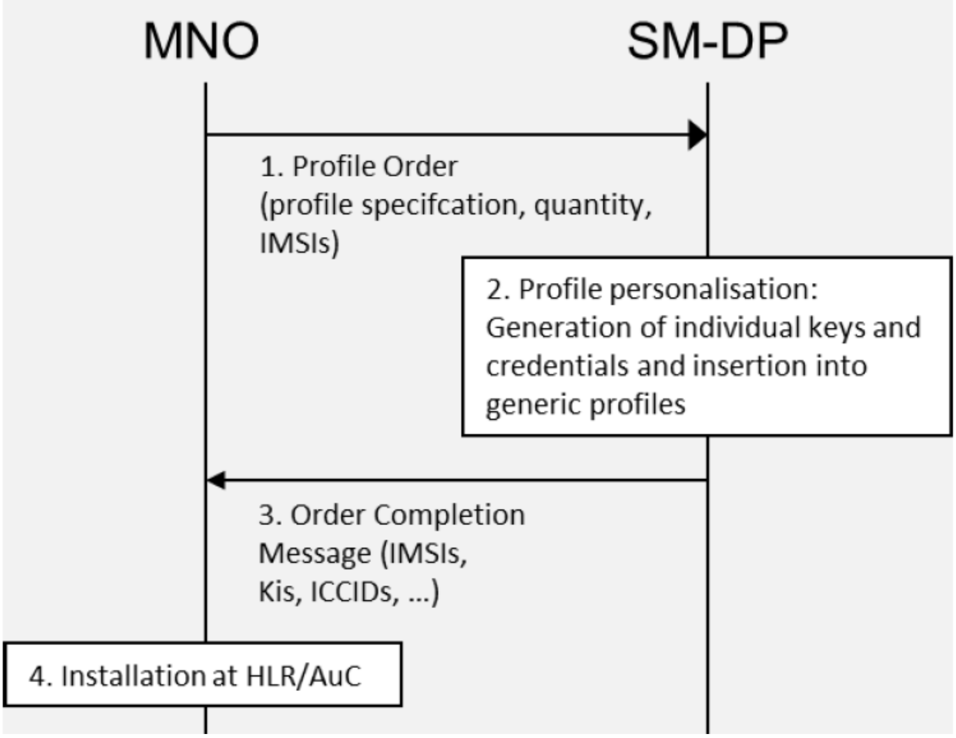
MNO
SM-DP
1. Profile Order
(profile specifcation, quantity,
IMSIs)
2. Profile personalisation:
Generation of individual keys and
credentials and insertion into
generic profiles
3. Order Completion
Message (IMSIs,
Kis, ICCIDs, ...)
4. Installation at HLR/AuC

Figure 3.7: Profile ordering [5]

downloaded and installed asks the SM-DP to enable it. The SM-DP identifies the SM-SR based on the information provided by MNO and where the eUICC is registered. The SM-DP and the SM-SR authenticate each other and the EIS requests from SM-SR by the SM-DP for a particular eUICC, and based on the EID the EIS retrieves by the SM-SR. the relevant information sends from the EIS from the SM-SR to the requesting SM-DP and based on this information, the SM-DP checks the eligibility of the eUICC. Then, if the problem of eligibility is detected, the SM-DP aborts the procedure and returns an error message to the SM-SR and the requesting MNO; otherwise the SM-DP issues an installation request for the ISD-P (Issuer Security Domain Profile) to the SM-SR.

An empty ISD-P is created in the eUICC when the SM-SR contacts the eUICC and confirmed back to the SM-DP. Therefore, a share key set is established between the ISD-P and the SM-DP, and SM-DP authenticates the eUICC. Between the eUICC and SM-SR a secure transport channel is established by asking the SM-DP from the SM-SR. The eUICC sends the result of the installation and state of the ISD-P to the SM-DP and then, SM-DP sends the result to the SM-SR. The SM-SR updates its database and inserts a new Profile record into the EIS, with the status ”disable” or ”enable” if the download and installation was successful. Finally, the SM-SR and SM-DP confirm the status of the download and installation back.

End Condition: An ISD-P has been created containing a profile in disable or enable in the eUICC for the MNO.

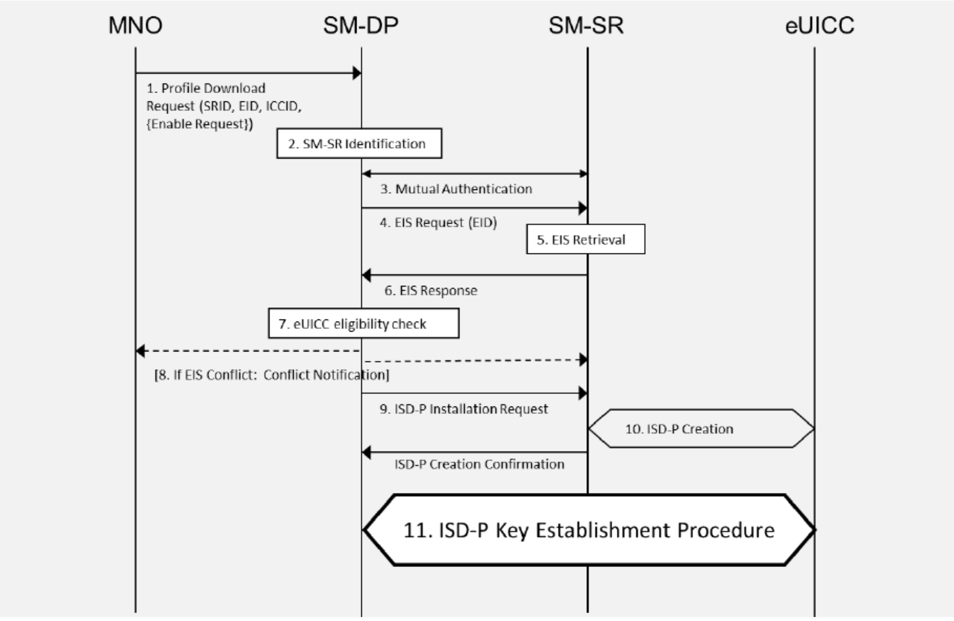
MNO
SM-DP
SM-SR
eUICC
1. Profile Download Request (SRID, EID, ICCID, {Enable Request})
2. SM-SR Identification
3. Mutual Authentication
4. EIS Request (EID)
5. EIS Retrieval
6. EIS Response
7. eUICC eligibility check
[8. If EIS Conflict: Conflict Notification]
9. ISD-P Installation Request
10. ISD-P Creation
ISD-P Creation Confirmation
11. ISD-P Key Establishment Procedure

Figure 3.8: Profile Download [5]

3.3.3.4 Profile Enabling

The following dedicated Figure 3.9 shows the procedure of a switch between two profiles. In this case the request is issued by the MNO with the target eUICC to the SM-SR.

Start Condition: The target Profile is disabled and the other Profile is enabled on the eUICC. The subscription associated with the target Profile and the EID, the

SRID and the ICCID of the target Profile are known and activated in the MNO's network.

Procedure: The enabling request sends by MNO to the SM-SR that includes the EID and at least the ICCID of the target Profile. The SM-SR checks to take place if the POL2 (Policy Rules associated to a Profile and stored in the relevant EIS at the SM-SR) of both the currently Enabled Profile and the target Profile permit the profile switch. The procedure will be aborted if there is a conflict with POL2. Otherwise, the SM-SR issues a Profile Enabling request to the eUICC of the target Profile and eUICC performs a POL1 (Policy Rules within the Profile) check.

The eUICC aborts the procedure and inform SM-SR if there is a conflict with POL1. Otherwise, if there is no conflict with the POL1, the previous Profile is disabled and the target Profile being enabled by the Profile switch resulting in the eUICC. The eUICC reports the result to the SM-SR and the SM-SR reports the Profile switch result back to the MNO. The messages will include the EID and the ICCID of their respective Profiles.

End Condition: The previously enabled Profile is disabled and the target Profile in enabled on the eUICC.

3.3.3.5 Profile Disabling

The Profile disabling procedure is shown in Figure 3.10.

Start Condition: The target Profile is enabled on the eUICC.

Procedure: The request for disabling Profile that includes the target EID and at least the ICCID of the target Profile is sent to the SM-SR by the MNO. Permission of the POL2 of the Enabled Profile to be disabled and permission of the POL2 of the provisioning Profile to be enabled will check with the SM-SR. If the target profile for disabling is the only profile existing in the eUICC, then the Profile disabling shall not be executed. The SM-SR aborts if the conflict happened and

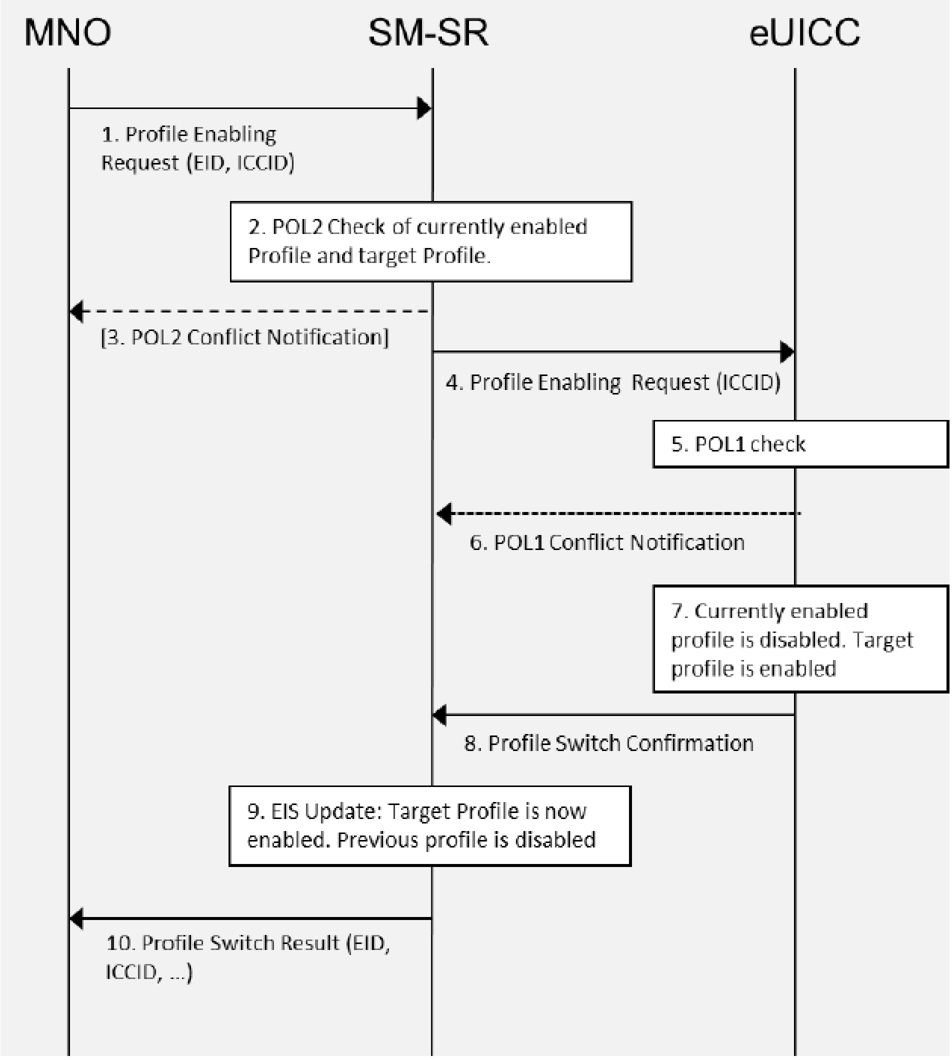
MNO
SM-SR
eUICC
1. Profile Enabling Request (EID, ICCID)
2. POL2 Check of currently enabled Profile and target Profile.
[3. POL2 Conflict Notification]
4. Profile Enabling Request (ICCID)
5. POL1 check
6. POL1 Conflict Notification
7. Currently enabled profile is disabled. Target profile is enabled
8. Profile Switch Confirmation
9. EIS Update: Target Profile is now enabled. Previous profile is disabled
10. Profile Switch Result (EID, ICCID, ...)

Figure 3.9: Profile Enabling [5]

send message to the MNO. But if there is no POL2 conflict, a provisioning Profile enabling request to the eUICC issues by the SM-SR. Therefore, the enabled Profile is disabled and the eUICC enables the provisioning Profile by checking an internal POL1. The result of the disabling Profile will report to the MNO by SM-SR.

End Condition: the provisioning Profile is enabled and the target Profile is disabled now.

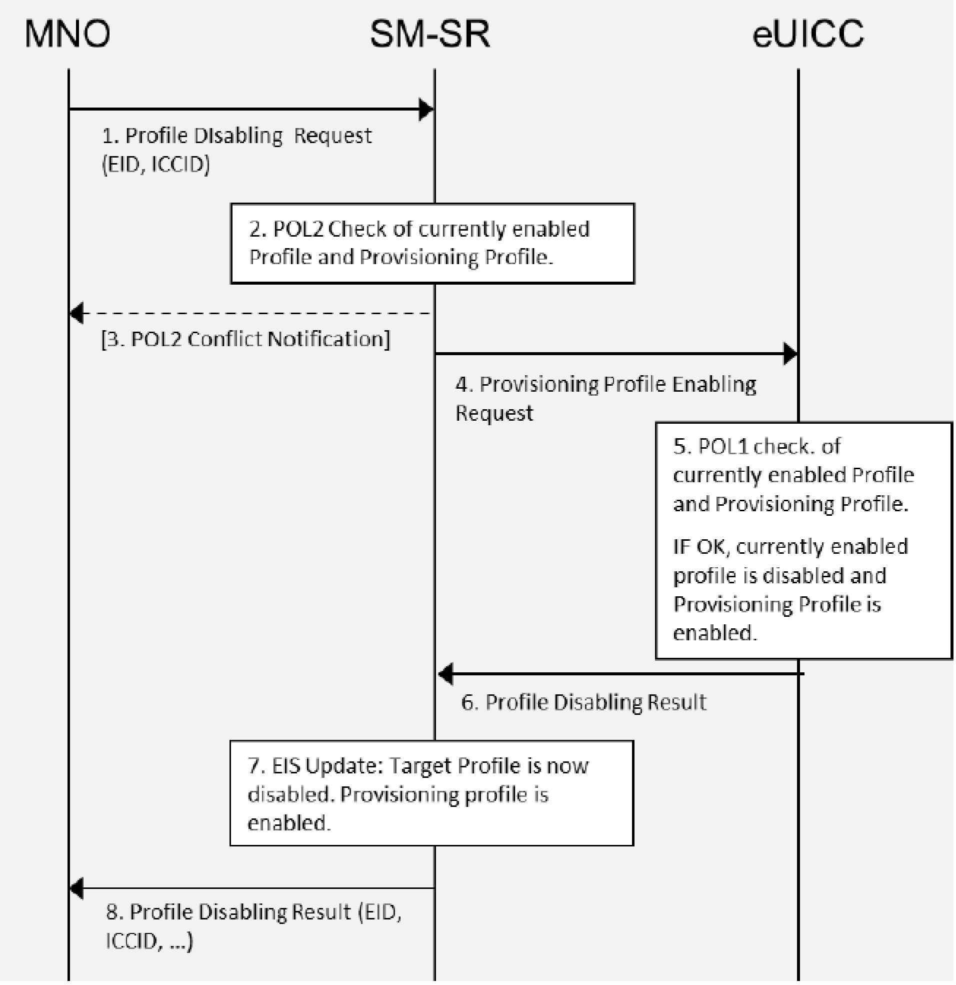
MNO
SM-SR
eUICC
1. Profile DIsabling Request (EID, ICCID)
2. POL2 Check of currently enabled Profile and Provisioning Profile.
[3. POL2 Conflict Notification]
4. Provisioning Profile Enabling Request
5. POL1 check. of currently enabled Profile and Provisioning Profile.
IF OK, currently enabled profile is disabled and Provisioning Profile is enabled.
6. Profile Disabling Result
7. EIS Update: Target Profile is now disabled. Provisioning profile is enabled.
8. Profile Disabling Result (EID, ICCID, ...)

Figure 3.10: Profile Disabling [5]

3.3.3.6 ISD-P Deletion

Figure 3.11 shows how a Profile can be deleted by its MNO.

Start Condition: The MNO decides to permanently delete a profile on a eU-

ICC.

Procedure: The MNO send request to delete an ISD-P to SM-SR and SM-SR starts the Profile Disabling procedure if the target Profile is enabled. Then, the ISD-P deletion request including the ICCID of the target profile sends to the eUICC. Therefore, the eUICC erases the related ISD-P and the target Profile, and sends the report to the SM-SR. Finally, the SM-SR updates the EIS appropriately and reports to the requesting MNO the status of the ISD-P deletion.

End Condition: The target Profile is deleted from the eUICC.

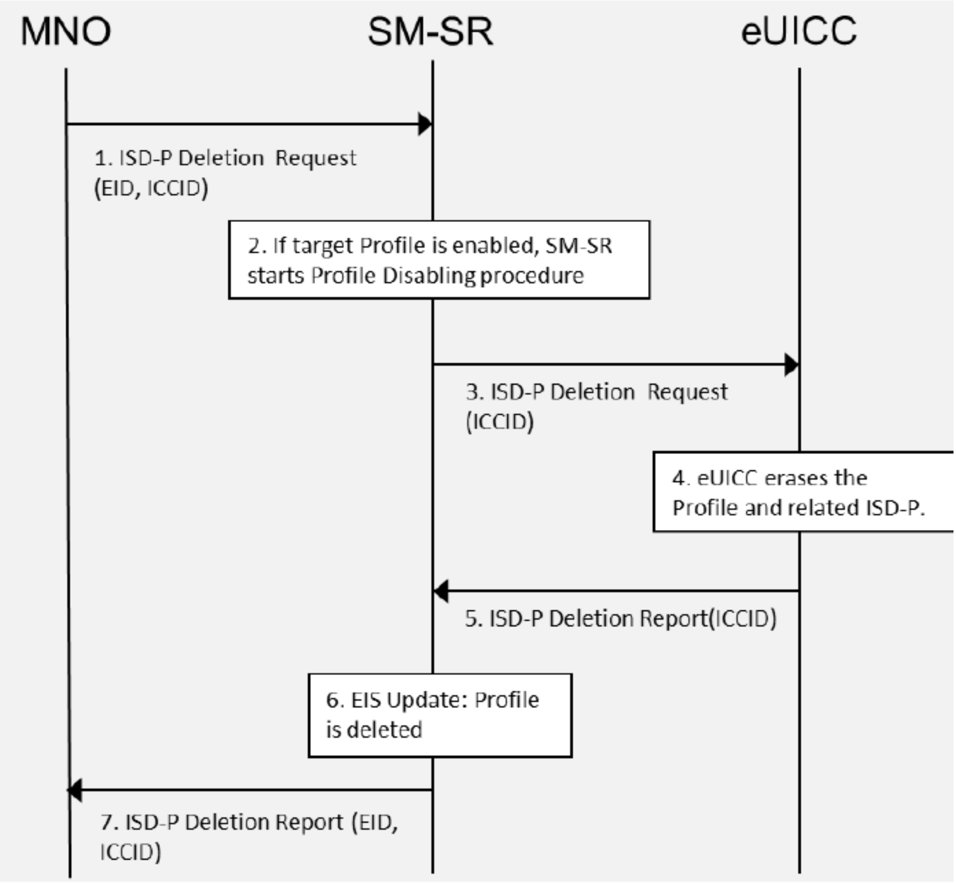
MNO
SM-SR
eUICC
1. ISD-P Deletion Request (EID, ICCID)
2. If target Profile is enabled, SM-SR starts Profile Disabling procedure
3. ISD-P Deletion Request (ICCID)
4. eUICC erases the Profile and related ISD-P.
5. ISD-P Deletion Report(ICCID)
6. EIS Update: Profile is deleted
7. ISD-P Deletion Report (EID, ICCID)

Figure 3.11: ISD-P Deletion [5]

3.4 Subscription Manager (SM)

The embedded UICC will be switched to personal terms and other data will be provisioned Over-the-Air. The remote provisioning is called Subscription Management. Therefore, for the soldered UICC with Subscription Manager there is an ability to change the SIM operator. Subscription manager [4] is a new role played by SIM venders from the management and manufacture of reprogrammable SIMs. The Subscription Manger is responsible for the secure process and technology via which a MNO is able to submit a profile to be loaded onto the eUICC.

Currently, the traditional SIM provisioning, MNOs send the vendors a file with their specifications, such as the IMSI numbers of the SIM cards and SIM venders send the personalized cards back to MNOs. MNO and SIM card vendors hold the relationship. Thus, only two entities are involved in the supply chain before the customer takes possession of the SIM card.

In order to be provisioned MNO's SIM profile to a SIM card after the SIM is delivered to the customer, a more complex process and ecosystem is required. Hence, the Subscription Manager dramatically reduces the complexity and increases the chance of success. Also without a Subscription Manager, the Embedded Service provides between each MNO. Each MNO would interface to Subscription Manager once and there would be only one Subscription Manager in an ideal technical. But for commercial reality requirements, one Subscription Manager is not a practical solution. Since MNO performing their own UICC personalization, could also performs much of the Subscription Manager Data Preparation (SM-DP) role themselves. The technical requirements are the same as other entity for a MNO to be Subscription Manager. However, they need to meet all the certification and assurance criteria that will be defined in the GSMA.

As describe by GSMA [3] in the eUICC ecosystem, a Subscription Manager is required that is fulfils by two functions; Secure Routing (SM-SR) and Data Preparation (SM-DP) in GSMA documentation on the high level architecture of eUICC.

3.4.1 Subscription Manager Data Preparation (SM-DP)

For the secure preparation of delivering package to the eUICC and for working with the SM-SR, SM-DP has responsibility. SM-DP includes following key functions:

- Certification level and functional characteristic will manage by SM-DP
- Managing the MNO credentials such as IMSI, K
- Computing the Over-the-Air packages for downloading by SM-SR

When a third party take on the responsibility of the SM-DP function role instead of MNO, the security and trust relationship are critical. Each MNO will have direct relationship with specific SM-DP.

3.4.2 Subscription Manager Secure Routing (SM-SR)

Secure routing and delivery of the credential package to the correct eUICC is doing by SM-SR. Performance, reliability and scalability requirements are expected to be significant for the SM-SR. SM-SR key functions include:

- The Over-the-Air communication manages by SM-SR through a ciphered VPN with the eUICC.
- Building end to end link up to the eUICC, require managing the communication with other SM-SR. (for example when MNO does not have a direct commercial relationship with the particular SM that manage that eUICC)
- SM-SR manage the eUICC data that is provided by eUICC suppliers and used for SM-SR OTA communication
- Protect communication with eUICC

Subscription Manager is changing operator depending on contractual state in accordance with the policy control function by allowing roaming agreements to other networks through a single profile. In the embedded SIM only one active profile and only connection to one network at any time are possible. Hence, multiple active SIM profiles will not supported. For example a eUICC that is concurrently active in more than one HLR are not possible, and allow clear customer responsibility and commercial relationship.

To ensure trust with Subscription Manager requires being certified using procedures similar to the GSMA security service that is performed on SIM vendors. Subscription Manager are only aware of credentials identifying the eUICC and don't hold any details of the subscriber.

3.4.3 Subscription Manager Requirements

The SM-SR and the SM-DP shall be certified according to a GSMA agreed certification scheme and implement an access control mechanism on the request for execution of the SMSR and the SMDP functions only to authorized security realms. Security realm of eUICC, SM-SR and SM-DP should have counter measure against denial of services attacks.

Finally, during the Profile installation which hosts the SM-DP function should be a secure end-to-end communication channel between the Security Realms.

At least one of the two mechanisms, Web Services Security standard (WS-standard) or Mutual Authentication Transport Level Security (SSL) is required to secure the message being sent between the entities. In the mutual authentication, the entities concerned to authenticate each other are SM-DP to SM-SR and SM-SR to SM-DP.

3.4.4 GSMA M2M Use Cases

For the successful development of an eUICC industry standard, GSMA [3] submitted a number of requirements and use cases document to ETSI to solve a problem specific to M2M devices, where changing SIM cards can be difficult and make a need of the remote management easier.

There are a total of 5 use case types that are the part of any subscription lifecycle. All Use Cases are required to support M2M or embedded service usage:

- **Use Case 1 - Provisioning of multiple M2M subscription**

  For a number of connected M2M devices, sets-up M2M subscription by a Machine-to-Machine Service Provider (M2M SP) that may later change subscriptions to a subsequent MNO.

- **Use Case 2 - Provisioning of first subscription with a new connected device**

  A subscriber purchases a new type of communications or connected device with a subscription to provide first services to this device from a device vender.

- **Use Case 3 - Subscription Change**

  A subscriber changes the subscription for a device in accordance with policy control functions for each MNO to stop services with the current MNO and start services with a new MNO.

- **Use Case 4 - Stop Subscription**

  A subscriber sells the device and stops the subscription from the current MNO for services.

- **Use Case 5 - Transfer Subscription**

  Subscriber transfers subscription between devices.

While there will be a range of consumer purchased devices for communication, some key technical requirements will become clear through examining a few examples with relevant Use Cases regarding the goal. Since GSMA Use Case 2 and 3 are more applicable to a consumer, are examined in more details below.

UC2a and UC2c from GSMA Use Case 2 and also UC3 are explained below. In the first alternative of GSMA Use Case 2, the MNO profile is provisioned to the eUICC after the customer has received it, and the second one is when the MNO profile is pre-provisioned.

As a further proof of concept, CSMG [18] developed a conceptual model of some Use Cases as shown in the following figures.

3.4.4.1 UC2a: Post-Provisioning of an eUICC

In this Use Case, the eUICC is programmed with an initial setup profile which enables to connect to the setup bearer (network) for initial OTA provisioning and download a selected MNO profile. The setup bearer profile would be written to an SSD. In this case, a consumer purchases a new device and subsequently selects the MNO. As shown in the Figure 3.12, the eUICC is divided into multiple part. The Issuer Security Domain (ISD) is the primary part and is controlled to creat, remove or share access to secondary security domains (SSDs). SSDs contain confidential data such as MNO subscription profiles. MNOs are able to access their own information such as IMSI, Ki, network security algorithms securely without accessibility by other MNOs.

Subscription Manager (SM) manages remote access to the eUICC on behalf of the eUICC Issuer. Secure Routing (SM-SR) function is responsible for management of eUICC.

The consumer can chose and setup MNO. The first provisioning of the eUICC, as shown in the Figure 3.13, can proceed when, the new profile request is sent from the eUICC to the Subscription Manager which forwards the request to the appropriate MNO. After checking validity by MNO, the MNO's Subscription Manager Data Preparation (SM-DP), prepares the appropriate MNO profile and encrypts it for eUICC.

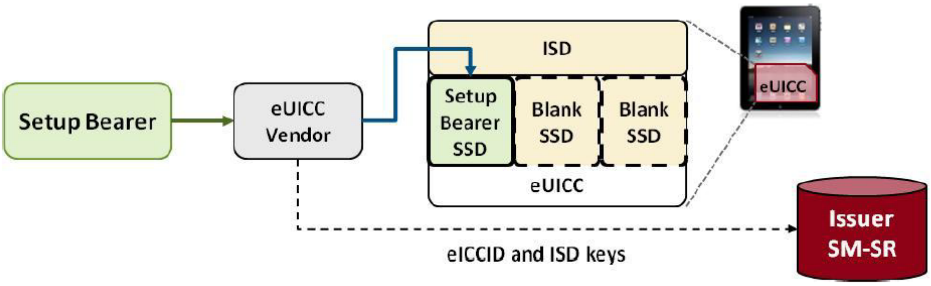

Figure 3.12: Provisioning of Setup Bearer to eUICC by eUICC vender [18]

The SM-DP is responsible for the secure assembly and encryption of the profile package to ensure that the MNO's secret data cannot be seen by the SM-SR or the eUICC Issuer, and securely sent OTA to the eUICC using the Setup Bearer's network as the provisioning network. Then the Subscription Manager client, contains in the eUICC, loads the package into the correct SSD and decrypts the package to install the new MNO profile on the eUICC. The SM client also activates the operational MNO profile and deactivates the Setup Bearer profile.

3.4.4.2 UC2c: Pre-Provisioning of an eUICC

Under this option, the customer has access to a valid MNO profile prior to the device purchase and customer would not need to select their MNO post-purchase. Also during the supply chain, the MNO profile is securely written to an SSD on

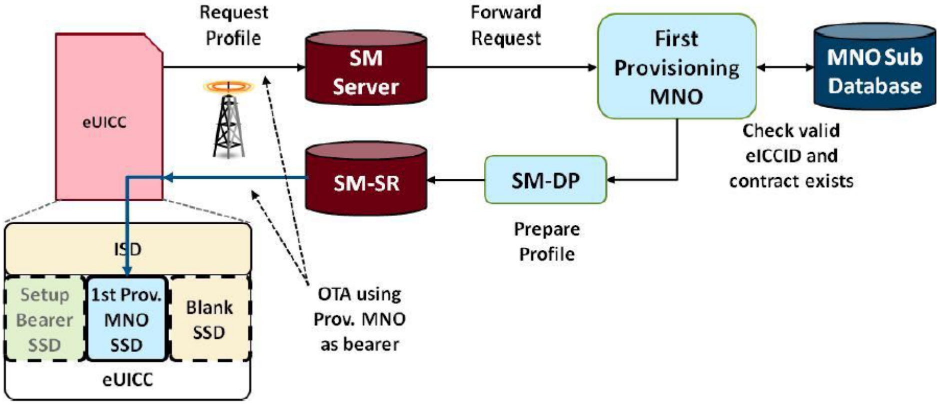

Figure 3.13: First Provisioning of Operational MNO to eUICC [18]

the eUICC and the eUICC Issuer would use an AM to manage and control access to the eUICC. (Figure 3.14)

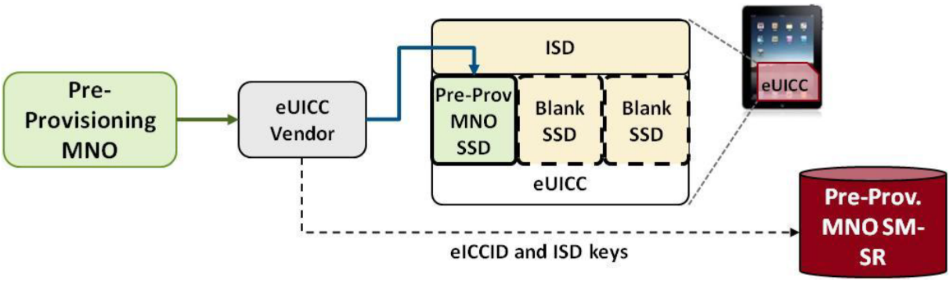

Figure 3.14: Pre-provisioning of eUICC by an MNO [18]

3.4.4.3 Switching of an eUICC between Operational MNOs

As describe in Figure 3.15, in this case, similar to the First Provisioning in UC2a, an additional Gaining MNO profile is installed on the eUICC beside the Losing MNO's profile. The eUICC request first is forwarded to the Losing MNO to validate the switching action against its policy control function, and then is sent to the Gaining MNO. Profile package is prepared and encrypted by SM-DP and is routed via the SM-SR on an OTA link to a new SSD on the eUICC. The OTA is expected occur over the Losing MNO bearer, so once the new profile is installed on the SSD, the

Gaining MNO profile is activated and the Losing MNO profile is deactivated.

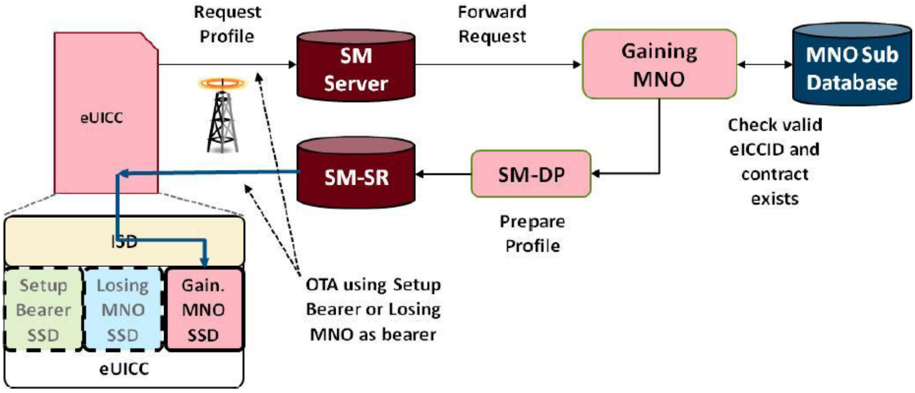

Figure 3.15: Switching of Operational MNOs on eUICC [18]

If an SM-SR is not connected to all MNOs, there is a potential issue of fragmentation. Therefore, SM-SRs develop technical relationship with MNOs in order to access to the market players. The eUICC can contain multiple profiles, but only one operational profile can be active at any point in time.

3.5 The evolution path 3: Soft-SIM

With the advances in wireless and technology has made it possible to have a Virtual SIM that can be provisioned as easily and cost effectively. There is also proposal to replace the current SIM by a tamper resistant module soldered on the mobile phone, also called Secure Element and software SIM downloadable over-the-air.

The term Soft-SIM has a particular meaning among some operators and SIM card manufactures, which is a virtualized SIM residing in handset memory. Due to extensive concern regarding the security of a Soft-SIM and the lack of MNO support of Soft-SIM, there is no widespread concern on their development and technologies.

Regarding to the challenges that was defined with GSM, for the third path of evolution i.e. Soft-SIM the machine will not be able to connect the mobile network because of lack of SIM unless by downloading SIM application over the air. In a soft SIM scenario it is typically the hardware platform that is responsible for protecting the SIM execution environment and credentials. Authorization is expected to be as for physical SIM enforced through the platform with hardware/software protection. It means protection is depending on their platform and their implementation.

The objective of this evolution path is reached when a chip (a Secure Element) with ability of dynamic downloading containing the SIM or USIM applications in terminal which is called Soft-SIM. The Secure Element is not an UICC but also use instead of UICC and it is a dynamic environment to store information and to download applications via a secure manner. The Secure Element is a smartcard module like a secure SD memory card soldered to the motherboard of terminal that could be part of microprocessor chip to install SIM application.

While current SIM cards still may be appropriate for complex devices, the cost associated with a SIM card may be preventively high for mobile devices. This new SIM form factor could be even more flexible and convenient for the users but it could be challenging to ensure the same level of security. It's not just consumers who stand to benefit, but also mobile networks are reaching remote geographies. The consumers would not have to worry about losing data and would never have to go to the operator's shop for a new SIM.

As rumored, Apple has been working with SIM vender Gemalto [31] to develop a wirelessly upgradable Soft-SIM and most importantly re-provisioned Over-the-Air, which wouldn't need a physical card at all in its devices.

Further, while future standards may require the same security functions implemented by customary SIM cards, such standards may not require an actual hardware implementation of SIM like SIM card. Thus, for the new technology we don't need to have initiate SIM and here is the different way of thinking that we should challenge and there remains a need for alternative SIM solution.

One would be where the reprogrammable SIM was pre-provisioned by the MNO that a consumer could therefore buy a handset with a reprogrammable SIM in it. In this case, handsets already have a particular MNO subscription on it. But under this option, the consumers would not select their need of MNO in the other area, and this option is not utilizable anymore in the Soft-SIM solution.

The GSMA requirements document also has described another alternative option that is the consumer buy a handset which has a blank reprogrammable SIM on it. In this case, the consumer would be able to select an operator at a later point in time, potentially using by downloading a particular MNO on a "blank" SIM. Since the write and read access to the eUICC can be done by restriction access to only authorized personnel, the challenge now is who can be defined as authorized personnel; The user, the mobile operator or owner of the equipment?

During SIM downloading, the most important issue is duplication and copying that may occur. Hence, another challenge is preventing the SIM to be copied and misused.

3.5.1 SOFT SIM alternatives

There are several Soft SIM alternatives [18]:

- **Apple Virtual SIM Patent**

  The architecture is based on the reprogrammable SIM architecture. The SIM application, which is provisioned by a Trusted Service Manager (TSM), holds on the device by the embedded secure element (SE). The MNOs may require in this solution to share certain information, such as the SIM profiles, with the handset vendors. As shown in Figure 3.16, Apple's "Virtual SIM" is located on the embedded secure element.

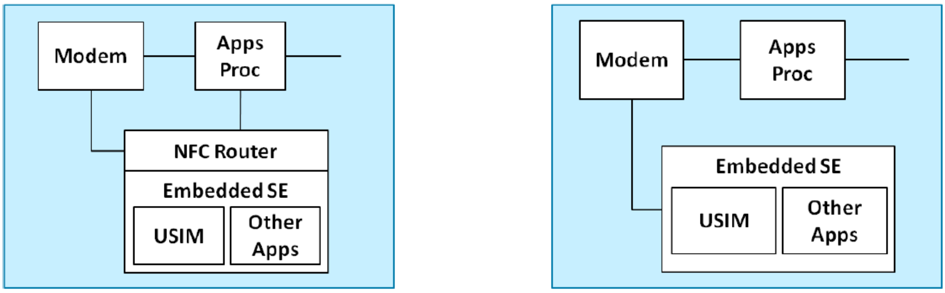

Figure 3.16: Apple Virtual SIM Architecture [18]

- **Truphone Patent**

  This patent shows the application of an international reprogrammable SIM which is considered by ETSI, and enables consumers to download a new IMSI if they are in a foreign country in order to avoid roaming rates.

- **Apple Patent**

This patent is not technically based on reprogrammable SIMs, but shows how devices may be able to switch network dynamically, in the same country with the MNO that providing the best cost and coverage at the time. The device is pre-programmed with an identifier (i.e. IMSI) which is used to recognize the identity and needs of the end-user with the Apple MVNO that has an HLR. Also the other components such as AUc, to be able to register the subscriber, are required.

In the Apple patent, the end-user maintains a single profile and networks switch when they have roaming agreements whereas in a reprogrammable SIM, an end-user could instead have multiple network operator profiles on the SIM, and in order to switch between network, swap between these profiles. Hence, this is a key difference between the Apple patent and a reprogrammable SIM implementation.

- **Qualcomm Patent**

In addition of three solutions that mentioned above, there is an example that show how a Virtualized SIM might work. Qualcomm [32] has been raised "Virtual SIM" patent solution that the GSMA has criticized as a "Soft-SIM". This concept, which is located on the handset memory, may potentially be enabled by advances in security technology such as the implementation of Trusted Execution Environments (TEE).

Qualcomm's Virtual SIM is positioned primarily as a subscription identity backup concept that is capable of reprogrammable SIM functionality. It enables user to backup SIM information for later retrieval to a Virtual SIM server. However, the Virtual SIM takes the place of a SIM card in GSM handsets. The Virtual SIM contains similar information that is used to authenticate with networks and store usage and provider data. In this case, instead of storing information in a SIM card, a mobile recalls the network provisioning information stored in the memory unit. Thus, consumers download this information into a new SIM card when they change SIMs or if they lose their mobile device and replace it with the new one.

A Use Case, the Virtual SIM service, is a "Soft-SIM" solution that can be used to provision a handset, and acts as the SM-SR and possibly SM-DP.

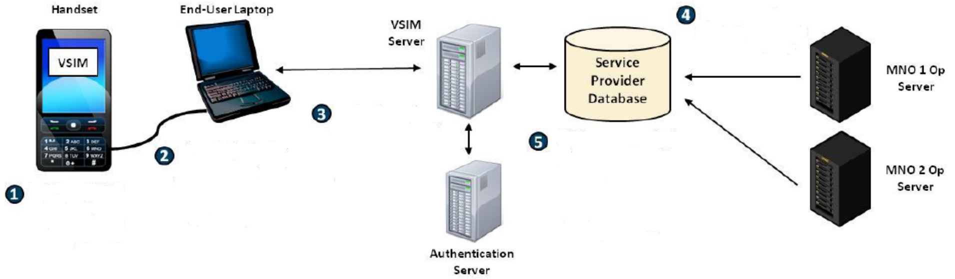

Figure 3.17: Qualcomm Patent Architecture [18]

Figure 3.17 shows the steps of application as follow [18]:

1. The Virtual SIM app on the handset will contain IMSI, Ki, VAS applications

2. Initial wired setup of Virtual SIM account includes download of SIM data to VSIM app; all new provisioning will be via wired connection

3. Backup and restoration activity requires Virtual SIM app on handset to be authenticated first

4. MNOs send subscription options to VSIM server

5. VSIM server can display MNO options to end-user from SP database and provision or switch subscription on an authenticated Virtual SIM when requested

3.6 Market Analysis

New market opportunities identified for the mobile industry particularly in the non-traditional industry by the GSMA market assessment. The GSMA market assessments also demonstrate new service concepts and development of design guidelines to promote common technology and operational solutions with the aim of reducing complexity and driving economies of scale.

As we know, numerous opportunities are opening up for vendors, system integrators, solution providers and MNOs regarding to an enormous market of devices. Usually, some operator business models are very much driven by subsidized devices.

The technology will give an opportunity for operators to provide more services and make their own decision to modeling in the business.

While the smartphones are increasing, growing data traffic is another major factor. With the increasing ubiquity of smartphones and availability of apps through app stores, mobile data is more resilient to price increases than mobile voice. However, due to increasing of bill shock and their increasingly public nature, bill shock is a current hot topic. Hence, implementing cheap mobile roaming facilities is a general hardening in the view. Then, data roaming is a major opportunity for operators. When consumers in the holiday, update their services and download data, make an opportunity for operator to sell data entertainment services via roaming cost.

Therefore, the devices containing embedded SIM or "Soft-SIM" with the ability of downloading SIM application Over-the-Air may not be such a bad architectural option for consumer. However, may the operators are privately saying that they could refuse to subsidize the device vendors (e.g. Apple) if insert an embedded subscriber identity module or "Soft-SIM".

Besides, the Mobile operators and payment card issuer may not agree on the new business model because they may not accept that their logo not appear on the physical card anymore. Also, at the moment the SIM comes from the mobile network operator with the full control over the access and billing, while new technology is not good news for operators and the mobile operator will no longer be 'in control'. The SIM card may continue to be made and used, but will become a low value commodity item.

One of the main issues that the telecoms industry must overcome is cost, in order to support and benefit from the emerging new technology markets. Regarding this, organizations such as GSMA and 3GPP have acknowledged and started several initiatives to address the issue. In the new business models and usage scenarios (e.g., downloadable SIM application), the user easily can access to several network whereas by installing physical SIM cards, the user is connected to the specific network and to change network has to fit another card in device. On the other hand, since issuing hard SIMs is expensive so the operators would save money by providing Soft-SIM, and downgrading the operator's connection with the consumer.

Apple proposed that in the future remotely program the SIM information by anyone to provide a service. In this case, since there is no any SIM card on the iphone, we will buy the handset and whole thing will be activated via iTunes and app stores cut the operators out from the business. Following on Apple's proposed, it has interest in reducing the size of SIM card or eliminating SIM cards entirely to save space, and allowing Apple to further shrink its devices or make room for other new components. The efforts led to Apple's proposal have been under review by the European Telecommunications Standards Institute (ETSI). To develop a Soft-SIM idea, Apple interested to work with Gemalto. Gemalto provides software solutions, Subscriber Identity Modules (SIMs) and manage services to subscribers in Telecommunications market. Also, it provides Secure Transactions and Security as well as functional organizations for marketing.

As long as operators are not ensure of the security credentials through the use of Soft-SIM and any compromise by operators could result in the loss of customer, they cannot easily accept having the third evolution. In order to promote of having third evolution, should provide a faster time to market with lower cost with the high performance and safety of the network. Obviously focusing on a well thought out and standardized solutions will much beneficial to achieve our goal. Certainly, several difficulty will need to be cleared and secured for a fair and comprehensive solution to arise, and thus we expect the Soft-SIM be a forcefully technology solution in the near future.

Chapter 4

Security Assessment of the SIM

4.1 Introduction

The other challenge in the new technology of SIM is security challenge. One of the important processes in security is an authentication concept. However, nowadays the term authentication is replaced by "electronic authentication" or "e-authentication". Regarding to the National Institute of Standards and Technology (NIST) [33] four authentication levels have defined as a technical guidance to implement electronic authentication which is useful mostly for example in smart card. Eavesdropper, replay, on- line guessing, man-in-the-middle and session hijacking attacks are prevented in these security authentication levels. Security levels also enable mutual authentication between parties which is very important to fulfill the requirements of security. In the end-to-end security solution without having the true ciphering key anybody cannot decrypt the transmitted data with a secure enough cryptographic algorithms which is deployed. SSL/TLS is one possibility to securing the communication channel.

Nowadays smartphones as communication tools has become important of particular concern as it relates to the security of personal information stored on smartphones. Indeed, increasing amount of sensitive information to access must be controlled to protect the privacy of the user and company. However, smartphones are applied different security counter-measure from security. Recently, the mobile industry also has experienced an excessive increase in number of its users. Therefore, with the greatest worldwide number of users surrender to several security vulnerabilities. Also communication parties become more vulnerable to the security threats with accessibility and openness of wireless communication.

Although, the GSM system also consider to the user authentication and Over-the-Air encryption in wireless communication, the solutions cannot be irrelevant with the new technology of software SIM. One of the practical scenarios can be deployed to misuse is Over-the-Air cracking. It is feasible to misuse when the IMSI and Ki of the target user be extracted without any physical access. Therefore, the attacker can clone the SIM and make and receive the information.

The point is that while the GSM network allows only one SIM to access to the network at any time so if the attackers try to access from different locations, the network will realize existence of duplicate cards and disables the affected account. The scenario can be similar to that one is explained in the following section for the secure transfer of software SIM. In the transferring SIM between two devices after establishing the secure connection and transferring SIM from transferring device to target device, transferring device send a deactivation message to deactivate and delete the Soft SIM in transferring device.

Indeed, if the technology and process of the SIM evolution were not defined with care, then it very likely would reduce security. Hence, focusing on standardized solution is more important than having fragmented property solutions.

In Chapter 2 security concept of current removable SIM is explained in details. Here focuses on second and third evolution of the SIM security.

4.2 eUICC security

4.2.1 Security in M2M System

The most important part of the Internet of Tings is the interconnection between the machines, which is called M2M, and it is widely used in power, public service management, transportation, industrial control, water, health, oil and other industries. Also it can achieve vehicle anti-theft, safety monitoring, public transport management and other functions. Hence, due to increasing attention to M2M in recent years, its development and character cause new security challenge. The most requirements of M2M are typically to be small, inexpensive, unattended by human and communicate over the wireless area network.

The three key factors vital for secure communications of Machine-to-Machine are:

- Authenticity - To assure the identity of the sender and recipient.
- Confidentiality - The inability for other individuals to eavesdrop the communication channel.
- Availability - The data services are usable by the appropriate in the manner intended.

M2M networks are more vulnerable to security threats due to longevity and field updates or provisioning. M2M components spend most of the time unattended and most of the communications are wireless, which makes eavesdropping extremely simple; and thus, it is easy to physically attack them.

Following attacks describe number of unique security vulnerabilities for M2M devices and the wireless communication network:

- **Physical attack**

  This attack may insert valid authentication tokens into a manipulated device. So, for the M2M device's software and data, trusted validation of the integrity and authentication tokens require.

- **Compromise of credentials**

  Comprising brute force attacks on authentication algorithms and tokens.

- **Configuration Attacks** Configuration attacks are such as fraudulent software update or configuration changes, mis-configuration by the owner, subscriber, user or compromise of the access control lists.
- **Protocol Attacks on the device** Major examples are man-in-the-middle attacks, denial-of- service (DoS) attacks
- **Attacks on the Core Network** These attacks are the main threats to the mobile network operator (MNO): DoS attacks against the core network.

They may also include changing the device's authorized physical location in an unauthorized fashion or attacks on the radio access network, using a rogue device.

- **User Data and Integrity Privacy Attacks**

  Other users or devices are eavesdropping when sent over the UTRAN or EUTRAN; masquerading as other user/subscribers device; users network ID or other confidential data revealed to unauthorized third parties.

An attacker can illegally access to the data on M2M device through eavesdropping user data, signaling data and control data on the wireless link in public place. Therefore, wireless link should be designed to prevent from eavesdropping or unauthorized accessing with two-way authentication mechanism of network and the corresponding encryption algorithm.

Damages can cause by attacker on the M2M user by modifying, inserting, replaying or deleting the legitimate M2M user data or signaling data transmission in wireless link. Thus, to reduce the damage on the network and to resist or mitigate the denial of service attacks, or tracking mechanism to quickly identify the location of attacker, M2M security system should be designed and ensured the network certification. M2M device should have special functions and related security mechanisms to prevent from steal or tamper with the user subscription information in. Therefore, by preventing the attacker logically or physically, the legitimate M2M users minimize the loss.

At the loss of legitimate users, Man-in-the -Middle attacks can steal or change the course of M2M communication of information between devices in the process of intercept data, modification of data and sending data. So, in order to obtain information, an attacker will obtain communication data in online listening, Man-in-the-Middle and any other ways.

Hence M2M equipments need to have integrity and confidentiality protection of data, and should have appropriate mechanism to perform this function.

The attacker is able to obtain user data through physical theft or online listening. So we can use the existing technology Trustchip[1], an embedded chip, to solve the secure communication between network systems and provides a singularly security architecture that operates as a security service to any application [34]. Therefore, to reduce the damage on the network, M2M security system should be designed to resist or relieve the denial of service attacks, or identify the location of attacker by tracking mechanism.

4.2.2 Security Requirements

In the security model we consider the MNO, Customer, SM-SR, SM-DP, eUICC and eUICC Manufacturer (EUM). They will be all belonging to a Security Realm [5]. Profile also shall be installs and load in a secure way. All cryptographic keys and the keys used by the EUM for eUICC Certificate generation shall be stored in a secure environment. The architecture shall provide a solution of its security principles of the global ecosystem, and to upgrade the network authentication algorithms used within the ecosystem. For the purpose of any communication, security shall be identifiable and mutually authenticated, and an entity may need authorization before communication exchange. The eUICC should be certificate according to the protection Profile defined in GSMA and compatible with existing accepted protection Profile. The eUICC also should be in line with Common Criteria EAL4+[2]and shall ensure of the complete clean of the profile within Profile deletion. Before installation in the eUICC the integrity should be ensured and the eUICC only accept the Profile sent from an authorized SM-SR and SM-DP.

To check identity and status will be expected a secure way for the SM-SR and SM-DP in such a way that the entity has a proof of identity and origin. Finally, the eUICC should reject any Profile Management command on the eUICC that is in conflict with the Policy Rules of any profile.

According to Embedded Mobile Guideline [6], since the technology of the GSM is fundamentally secure and embedded services offer an unequaled level of security, but still require considering key security issues. The following is high level guideline:

- Tampering and theft
- Malware
- Diagnosis and privacy

[1] TrustChip provides an end-to-end mobile protection - from the originating device, through the network, to the destination device.

[2] ELA4+ is the forth level of the Evaluation Assurance Level which is following the completion of a security evaluation.

- Unique IMEIs
- Firewall updates
- Credentials

EM device and application developers should provide the owner of data and consider how the transfer of personal data will be performed and secured, and what encryption mechanisms are appropriate.

EM device will often are more vulnerable to tampering. For example in the traditional mobile device in order to steal mobile service an attacker may be motivated to tamper by removing and using U(SIM) in another mobile device. However, with an EM device, unauthorized use of EM device may go unnoticed for longer compare to traditional mobile device. To prevent unauthorized access to network and systems, fraud management for EM applications relies on a combination of business processes and security measures are required.

In order to minimize the risk of the U(SIM) from the EM device being used for theft of service, the MNO observe to some fraud management. The following recommend some fraud management:

- The EM application restrict services to the minimum
- Limit traffic volumes that might be required for application
- Restrict IMSIs to work only with specific range of IMSIs
- Securely provision EM applications through the use of IPSec

To secure the smart card and to help ensure the integrity of the smart card used in EM applications and its authentication data under the GSMA Security Accreditation Scheme, it is essential that the supplier-side manufacturing environment is secure.

4.3 Soft-SIM security

Since the concept of Soft-SIM is downloading SIM application over-the-Air via a secure connection, encrypting the backbone traffic can prevent eavesdropping or modifying information by attacker between the network components.

The other solution can be End-to-End security or the application layer security solution that is more important and profitable. It can be provided in the cellular systems by one or some of following approaches [35]:

1. Using the programming languages such as J2ME (Java 2 Mobile Edition) in the mobile phone
2. Capabilities of the SIM using the SIM Application Toolkit (SAT)
3. Exploiting the processing capabilities of an additional smart card e.g. JavaCard
4. Capabilities of a PC to the ME
5. Capabilities of a crypto processor that is embedded in the ME

4.3.1 Wireless Network Authentication

The purpose of this solution which is invented by Schell.S et al. [2] and proposed by Apple, is allowing user devices to authenticate to wireless networks (e.g. cellular networks) by using access control clients. This technology can be one of the solutions in Soft-SIM authentication.

However, Subscription Identity Module (SIM) card includes security information that can be used in authenticating user equipment to a cellular network, but it may not always requiring SIM card. Even, SIM card make a device bulky and add cost. It would therefore be able to management of SIM by the manufacturer or service provider, and to provide users with the ability to use wireless network services. A cellular telephone company, a network service provider, may distribute access client (e.g. Universal Subscriber Identity Module (USIM)) to Trusted Service Manager (TSM) via a USIM vendor or directly.

The TSM (e.g. Apple's iTunes) maintain a list of authorized users, customer of TSM or an associated entity. The TSM provide the user with a set of USIM credentials that is stored in a Secure Element (SE) on the user equipment. Thus, the user equipment uses the USIM credentials that are stored in the SE to authenticate to the network service provider.

The invention is useful for both current art architectures (e.g., USIM data in a physical SIM card), and new architectures (e.g., USIM data stored in a secure element). SIM data includes high useful security contents for authentication such as key and encryption algorithms and also may contains user information such as identification information, network selection parameters, operator data and application data.

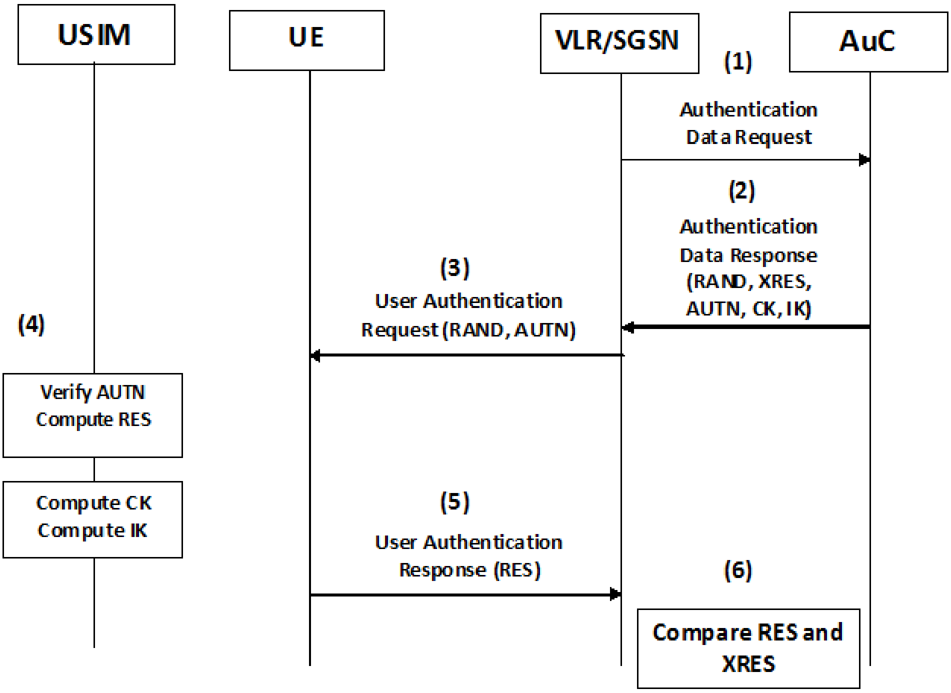
USIM
UE
VLR/SGSN
AuC
(1)
Authentication Data Request
(2)
Authentication Data Response (RAND, XRES, AUTN, CK, IK)
(3)
User Authentication Request (RAND, AUTN)
(4)
Verify AUTN Compute RES
Compute CK Compute IK
(5)
User Authentication Response (RES)
(6)
Compare RES and XRES

Figure 4.1: A prior art Authentication and Key Agreement (AKA) procedure [2]

Figure 4.1 illustrate a current art authentication procedures and key agreement procedures in the cellular system. During authentication, first UE receives the IMSI from the USIM and passes it to the Service Network (SN) of the network operator or the visited network. Then the authentication request forwards by the SN to the AuC of the Home Network (HN). The appropriate K obtains when the HN compares the received IMSI with the AuC's registry. The random number (RAND) generates by HN and signs with K to create the expected response (XRES). For use in cipher and integrity protection as well as Authentication Token (AUTN), the HN generates a cipher key (CK) and Integrity Key (IK) and sends an authentication vector. The Authentication vector consist if RAND, XRES, CK, and AUTN. For one-time authentication process the SN stores the Authentication vector and passes the RAND and AUTN to the UE. The USIM check the validity of AUTN by receiving the RAND and AUTN. Then, the UE compute its own response (RES) using the same algorithm that generated the XRES, received RAND and stored K, and passes the RES back to the SN. Finally, Service Network compares the XRES to the received RES, and authorizes the UE to use the operator's wireless network services when they match.

Conventionally, the USIM data authorize users in the form of SIM cards and generally requires the availability of a SIM card slot in the user's equipment. But in the new technology, as shown in the User Equipment part of Figure 4.2, a USIM sores within an embedded Secure Element not a removable card. However, it is not necessary for the user equipment to receive the USIM data in the form of a removable SIM card. The USIM data may be distributed using wired and/or wireless network connection via network service provider directly or using USIM vender and/or Trusted Service Manager. Usually the Trusted Service Manager, an organization that sells user equipment, maintains a database of user credentials to establish which users are of the TSM and are authorized to obtain network access from the network service provider. The users of the User Equipment establish account information that included in the user credential when purchasing the UE. The account information is inclusive of username, password, credit card information, and other information that may be used to establish the identity of authorized users.

As shown in the Figure 4.3 with the present invention by Schell.S et al. [2], USIM data is generated at an operator and distributed to a USIM vender. The USIMs can transfer to a Trusted Services Manager (TSM) by the USIM vender. Afterward, the TSM provides the USIM over any secure channel (e.g., wireless or wired interface) to a cellular device into the Secure Element. The steps of activation, authentication and registration occur when the USIM successfully transferred to the cellular device and operator.

4.3.2 Secure Transfer

Generally the SIM card which is contains the SIM application, subscriber details, and security information that a person owning multiple mobile devices manually moves the SIM card from one terminal to another. Thus, when a secure element

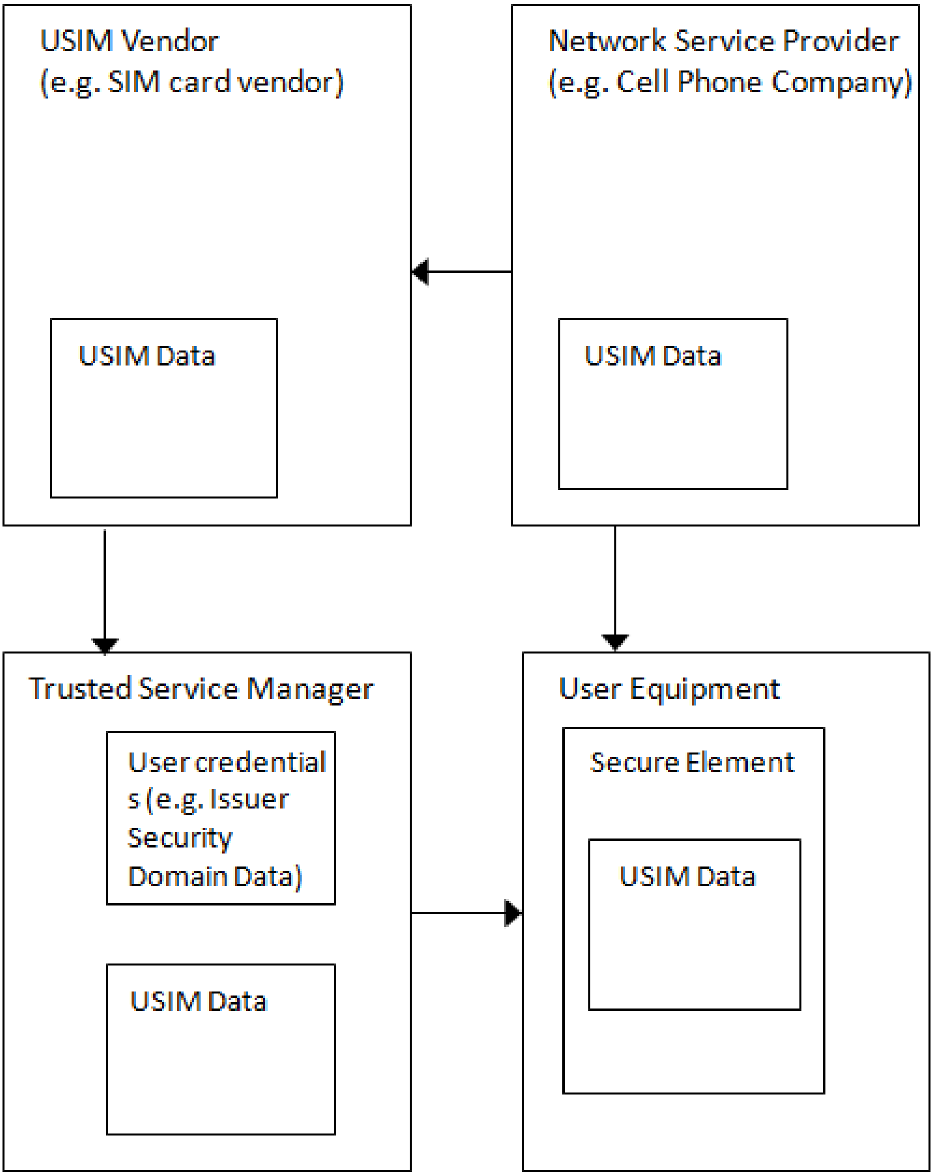

Figure 4.2: A diagram of an illustrative wireless system [2]

containing SIM application is soldered onto the mobile phone, it is not possible to physically change the secure element from a mobile phone to another one.

Chatrath [36] and Gehrmann [1] have proposed some solutions regarding to

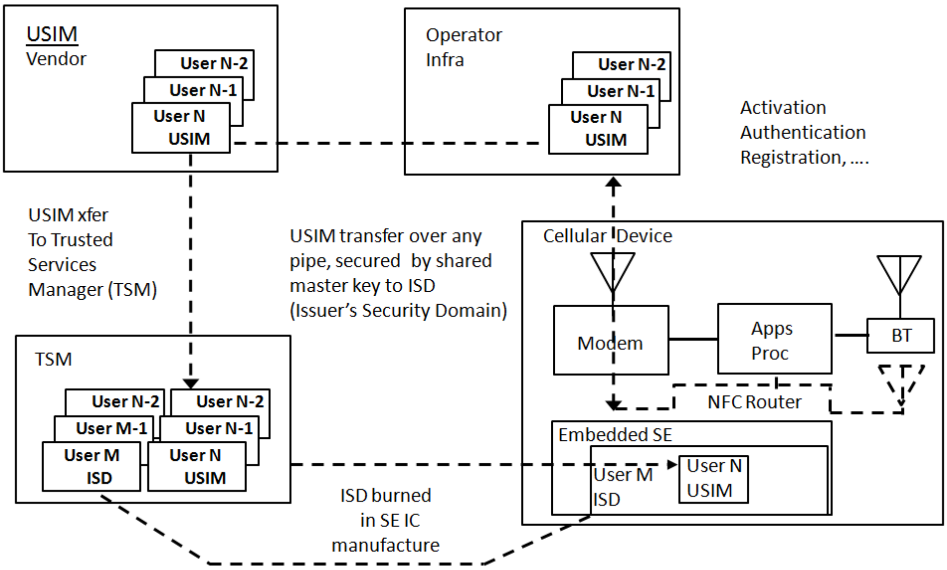

Figure 4.3: The method for deploying USIM information to a cellular device [2]

transferring software SIM in their patent. Chatrath described the mechanisms that can be used when a user can transfer the soft SIM to the new terminal when a new device is purchased.

Figure 4.4 illustrates soft SIM components that be contained in a memory of a device used for communication and the SIM information stored in a software file in terminal or soft SIM instead of the SIM information being stored in a hard module. The device also includes a CPU (Central Processing Unit) and an I/O (input/Output) module.

In this scenario there are multiple handsets with one soft SIM. When a user buys a new ”SIMless” terminal, the soft SIM can transfer to the new terminal and new terminal become active and the others become passive. The soft SIM is divided into a SIM Standard Component (SSC) and a SIM Active Component (SAC) in order to limit the size of the file transfer from one terminal to another. The SSC contains information to make successful connection between the terminal and the network. On the other hand the terminal has a unique SAC to define whether a terminal is active or passive. The both components can be contained in a module and encrypted to protect the information contained therein.

Due to some reason transferring maybe required, and a number of scenarios can

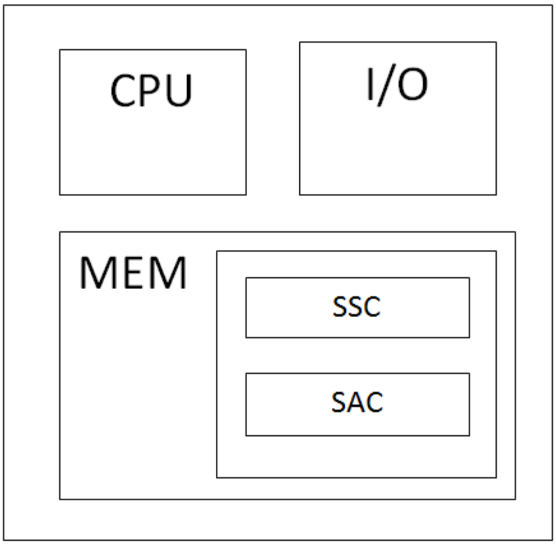

Figure 4.4: Components of a software SIM [36]

arise where credentials are required to be moved from device A to device B. but the main goal to bring this procedure is showing the secure transferring of software SIM between devices.

This part relates more particularly to the secure transfer of soft SIMs and the method of transferring from transferring mobile device to a target mobile device either directly or via a network server when only one mobile device contains active Soft-SIM at a time. SSIM may contain other SIM data like personal information about the user associated with the SSIM.

Figure 4.5 describes the peer-to-peer Soft-SIM transfer process directly to a target mobile device including all secret parameters with a complete SIM subscription. The process will happened when ensuring that only one of the mobile devices holds a valid and active SSIM at any given time [1]. Mobile devices communicate with each other including local connection over a communication channel using wired or wireless connection. Local connection can be cellular or internet connection.

The SIM unit of the target mobile device verifies the authenticity of the received SSIM. The transfer request includes the identifier (ID) of the trusted authority. If the target SIM unit trusts the authority identified by ID, the target SIM accepts and installs the SSIM and sends an installation ready message to the transferring device.

Private and public key pair may associate with the Soft-SIM. The transferring SIM unit may further encrypt SSIM using the target device's public key and the target SIM may decrypt, verifies and installs the received SSIM.

Hence, a secure connection is established between the transferring and target mobile devices according to the Transport Layer Security (TLS) [37] protocol or the Internet key Exchange/IP security [38] protocol. Subsequently, the transferring mobile device sends a deactivation complete message to the target and deactivates the SSIM in its SIM. Then, the target mobile device's SIM activate its SIM and sends an activation complete message. Thus, the transferring mobile device deletes the SSIM stored in SIM unit.

All message exchange protect by the secure connection using mutual authentication, key agreement, and/or confidentiality and integrity protection [1].

The peer-to-peer transfer process is fairly robust. For example, if the connection is broken, the target SIM unit may request a retransfer of SSIM.

In each mobile devices, the SIM unit may contains sensitive information related with the mobile device or and/or SIM credential. For example, the SIM unit may contain, manufacturer of the mobile device or a third party certification authority.

Figure 4.6 describes implementing a network assisted transfer of Soft-SIM from a transferring mobile device to a target mobile device including all secret parameters with a complete SIM subscription. The process includes a network server, e.g., a subscriber server. The connection may consist of any type of wired or wireless connection, including network base such as, cellular or Internet connection using any known securing process.

As we have described in the peer-to-peer Soft-SIM transfer, the secure connection protects all message exchanged between the transferring mobile devices and the network server using mutual authentication, key agreement, and/or confidentiality and integrity protection. The transferring SIM unit may accept or reject the request from target device by confirming the authority. The transferring mobile device establishes a secure connection for example, according to Transport Layer Security (TLS) protocol or the Internet Key Exchange/IP security protocol. If the SSIM transfer request accepted by the network server, the network server deactivates the SSIM and sends a deactivation message to the transferring SIM unit.

The transferring mobile device may encrypt the SSIM, and send the encrypted

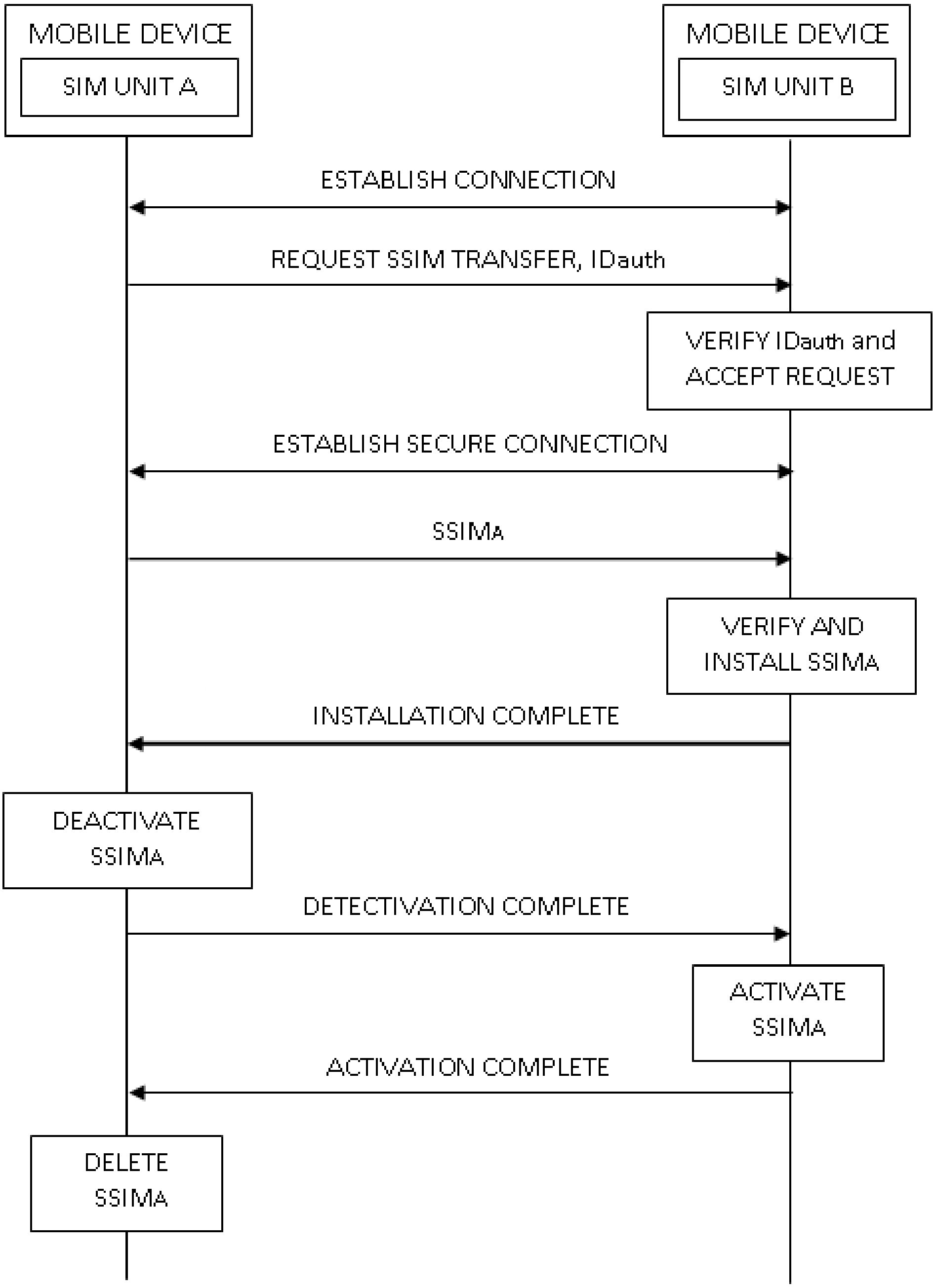

Figure 4.5: process diagram for a peer-to-peer transfer of Soft SIM [1]

SSIM over a non-secure channel to the network server. The network server also may protect the activated SSIM using an encryption by sending over a secure channel established between the network server and the target mobile device. Subsequently, the target SIM unit decrypts and installs the activated SSIM and sends an acknowledgment to the network server. The network server attempts to resend the protected SSIM when the connection is broken, also network server requests an update on the installation process. Figure 4.6 shows the transaction in details.

The above scenario, while ensuring that only one mobile device has a valid and active Soft-SIM at a time, eliminating the need for hardware-based SIM technology will possible. Further, there will be a way for future communication protocols that don't required hardware SIM card.

4.3.3 Trusted Execution Environment (TEE)

A Trusted Execution Environment (TEE) is a secure area to ensure that sensitive data is stored in the main processor of smart phone and mobile device and offers a Trusted Applications to provide end-to-end security by administrating protection, integrity, confidentiality and data access rights. Device manufacturers, Mobile Network Operators (MNO), application developers and platform providers and silicon vendors are all interest to have secure implementation and document standard. To make up the security framework within a mobile phone, there are three mobile environments [33]:

- Rich Operating System (Rich OS): Device applications are executed in this environment which is open to third party download after the device is manufactured.

- Trusted Execution Environment (TEE): The TEE is an essential part of the mobile ecosystem and generated in the Rich OS environment and offers a level of protection against software attacks. It is making up of software and hardware.

- Secure Element (SE): The SE allows high levels of security and is included of software and tamper resistant hardware and filters access to applications stored directly on the SE. The SE is mandatory for payment applications or electronic signatures.

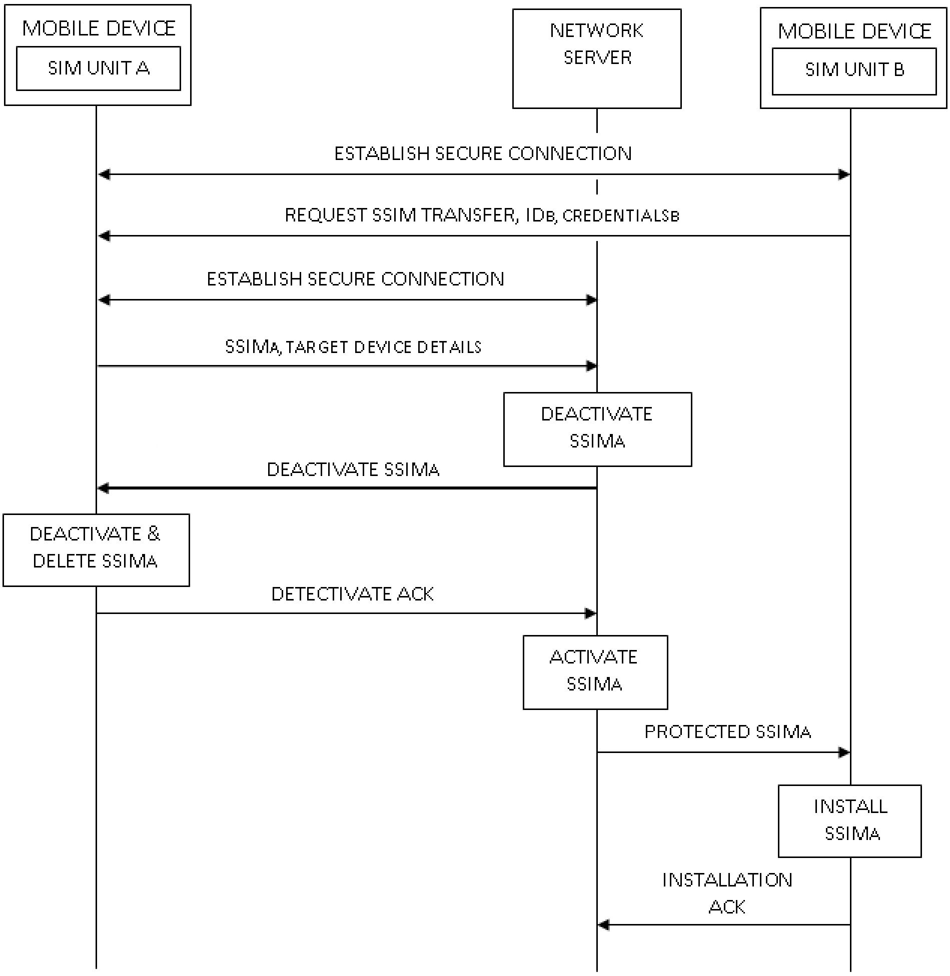

Figure 4.6: process diagram for a network based transfer of Soft-SIM [1]

By increasing the number of user, there is a need for protection from malware and attacker. So mobile services are required a greater level of security in applications much more than what offered by software solutions alone. The TEE environment also provides satisfaction for the business requirements of different content providers. For providing higher services to customers, MNOs also need TEE to facilitate increased revenues.

A Trusted Execution Environment (TEE) as illustrated in the Figure 4.6 [18], enhances the security of a reprogrammable SIM application (e.g. a "Soft-SIM") running on the handset memory or a separate secure element.

TEE could make SIM application more secure to communicate with secure services and uses secure drivers and interfaces that link hardware security features to the TEE environment. While, the GSMA has previously criticized the concept of "Soft-SIM" is being insecure.

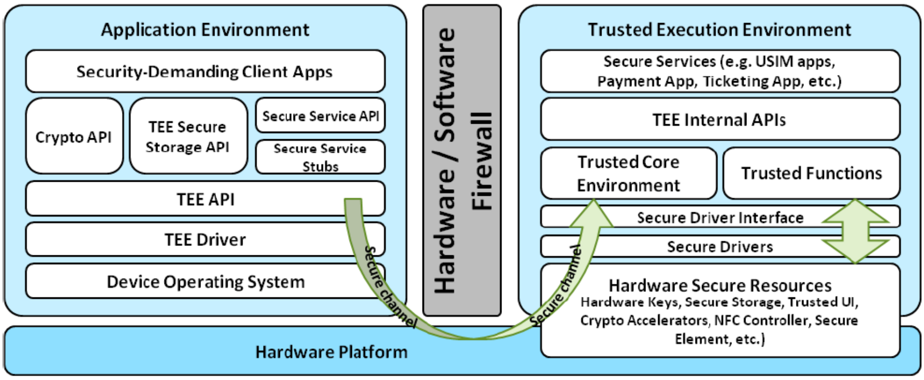
Application Environment
Security-Demanding Client Apps
Crypto API
TEE Secure Storage API
Secure Service API
Secure Service Stubs
TEE API
TEE Driver
Device Operating System
Hardware / Software Firewall
Trusted Execution Environment
Secure Services (e.g. USIM apps, Payment App, Ticketing App, etc.)
TEE Internal APIs
Trusted Core Environment
Trusted Functions
Secure Driver Interface
Secure Drivers
Hardware Secure Resources
Hardware Keys, Secure Storage, Trusted UI, Crypto Accelerators, NFC Controller, Secure Element, etc.)
Secure channel
Secure channel
Hardware Platform

Figure 4.7: Application and Trusted Execution Environment [18]

4.3.4 Trusted Environment (TRE)

A Trusted Environment (TRE) provides a hardware security anchor and root of trust (RoT). The TRE contains all necessary resources to provide a reliable environment and protect the system behavior for the execution of software, and storage of sensitive data. The internal system operations secure by RoT [34]. The authentication data store inside the TRE to provide protection function for the authentication of the device towards the operator's network. It could also make SIM application, to securely communicate with secure devices (e.g. payment and ticketing application).

4.3.5 Secure Element(SE)

Data and applications store in the secure element to access via a secure manner. The secure element is a smart card module (USIM, embedded secure element or separate secure element like a secure SD memory card).

The secure element is a dynamic environment to store information to authenticate the user in the network. In the secure element applications are downloaded, personalized, managed and removed independently. The secure element also has possibility to remotely lock in case of loss or theft. Madlmayr et al. explained that when secure element is used of a separate chip in the mobile phone, the biggest problem probably is transferring to the other device [39]. However, the SIM card that is already a removable secure element in the mobile phone with all data and features, can moves to the other device. Although the cost of a ”built in” secure element is lower than the cost of a removable one. The usability of built-in secure element is explained in the secure transfer section.

4.3.6 Trust Zone

Trust zone provides a secure hardware execution zone and memory partitioning. This technology may make possible to have security in downloadable SIM that is replacing with physical SIM card. Many silicon vendors are licensing Trust Zune which is possible to secure auxiliary equipments to ensure they can be protected from software attack. Therefore, this technology provides a programmers model across vendors, platforms, and applications to provide a security environment.

4.3.7 Trusted Service Manager

Account information get inside all mobile devices for getting new or updated account information. This is involves a new kind of provisioning role called Trusted Service Manager (TSM). The TSM provides business services, customer services and quality assurance. It also manages relationships between service providers and mobile network operators. The TSM has ability to manage ”many-to-many” relationships across multiple service providers and multiple MNOs. The following Figure 4.8 illustrates the essential tasks of the TSM into four broad areas of interdependent activities. The TSM also must be able first-time provisioning of new applications to a secure element and post-issuance updates and content delivery for over-the-air (OTA) provisioning across different MNOs.

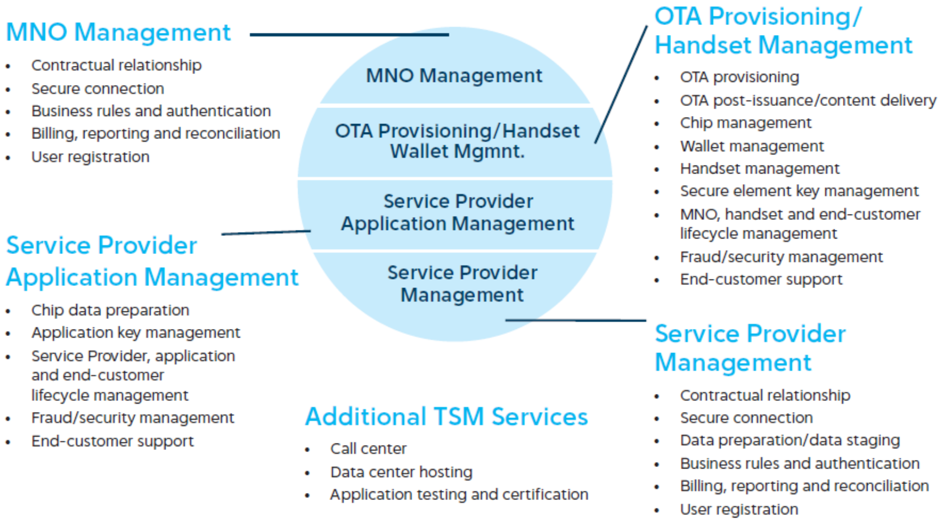
MNO Management
Contractual relationship
Secure connection
Business rules and authentication
Billing, reporting and reconciliation
User registration
MNO Management
OTA Provisioning/Handset Wallet Mgmnt.
Service Provider Application Management
Service Provider Management
OTA Provisioning/ Handset Management
OTA provisioning
OTA post-issuance/content delivery
Chip management
Wallet management
Handset management
Secure element key management
MNO, handset and end-customer lifecycle management
Fraud/security management
End-customer support
Service Provider Application Management
Chip data preparation
Application key management
Service Provider, application and end-customer lifecycle management
Fraud/security management
End-customer support
Service Provider Management
Contractual relationship
Secure connection
Data preparation/data staging
Business rules and authentication
Billing, reporting and reconciliation
User registration
Additional TSM Services
Call center
Data center hosting
Application testing and certification

Figure 4.8: The essential tasks of the Trusted Service Manager [40]

4.4 Security improvement in the Reprogrammable SIM

In order to improve the security of the end user of a terminal during transferring SIM application, several improvements are proposed. Merrien.L et al. [41] propose several improvements related to the management of secure element in the reprogrammable SIM. The five improvements explain as follow:

1. Generally the SIM card which is contains SIM application and a small circuit board can moves manually by owner of multiple terminal from one terminal to another. Thus, there is a need for owner of device when secure element is soldered onto the mobile phone to transfer SIM application between devices.

   For this purpose the first improvement concerns the authentication of the end user of the terminal. The downloading SIM application from the first secure element must be secured, meaning, ciphered in order than only the target secure element able to read. The SIM application then can be reinstalled on another secure element and sign in order to ensure that the package comes from the initial secure element. The SIM application can install after security checking by the target secure element. In this process imaging that the end user is entering a secret key to authenticate himself and to confirm the operation. In order to avoid of a problem, it could be possible to request for authentication.

2. The second improvement concerns a way when user wants to secure its sensitive data and keys before buying new terminal. The old and the new terminal may are not available at the same time. When the secure component is removable i.e. UICC in SIM card, then user can just remove the secure component. But if the UICC is not removable i.e. secure element so, it is another problem that arises in the case of secure element. To this purpose, the sensitive data export to a secure server for further download into another terminal. The advantage of this improvement is that there is no risk of losing the data.

3. The next problem arises when the device is infected by a malware. In this case the embedded UICC or secure element needs to be maintained during their whole life which consists remote update of the secure element content. Therefore, the improvement relates to the remote management and performs by a remote administration platform to manage through a potentially unsecured network and an unsecured device with an attached secure element. Malware can be existed at the level of Internet or at the level of the device. There is usually an end-to-end secure communication protocol between the secure element and the administration platform to have secure process. It means in most cases there is some middleware on the device that initiates the secure administration session and has to be secured with e.g. TLS for authentication of remote management request, avoiding denial of service, confidentiality of the request, etc.

   The mentioned management consist at least one of the following tasks:

   - Downloading content on the secure element
   - Deleting content on the secure element
   - Exporting content stored on the secure element
   - Activating content stored on the secure element
   - Deactivating content stored on the secure element

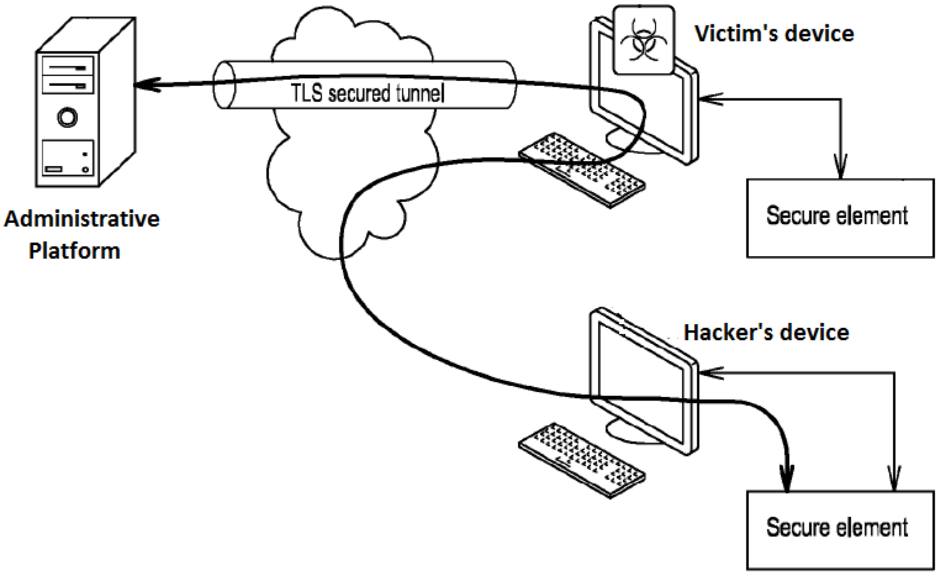

Figure 4.9: Diagram of the system with a hacker's device [41]

As figure 3 shows, some malware is located on a terminal even if the channel is secured through TLS and the credential used to authenticate the device stolen by the malware. The data can direct to another secure element located in a hacker's terminal through the Internet instead of the owner of terminal. In this procedure, the owner of terminal asks for subscription to a given MNO through the Internet from the administrative platform and prepares the content to be downloaded including SIM application, IMSI, Ki, etc. This process and redirection can be very harmful especially in the Telecom domain when entire SIM application is downloading on the secure element of the hacker. In this case, the owner of terminal not only not be able to connect to this MNO's network but also should pay for hacker's communications.

4. The next improvement is considered to reduce personalization cost in factories and allows owner of terminal to update the personalization of a secure element without need to go to the service provider shop. In this improvement process end-user allows to personalize secure element by transferring data on it.

5. Today, in the removable SIM when customer buys a SIM card, all confiden-

tial data such as PIN and PUK are delivered to the customer. The fifth improvement is the ability of end user to read securely the personalization confidential that are stored in the embedded UICC same as what it is in the removable UICC.

Chapter 5

Conclusion

Current SIM cards provide flexibility and security in subscriber authentication which satisfy the need of operators and users. The subscription profile used in a device also can be easily changed, by swapping the physical SIM card. The user's credentials in the current removable SIM are very well protected and it is almost impossible to extract the secret key with newer authentication algorithms.

However with the emergence of M2M communication, where devices are communicating through the mobile network, new demands have arisen. Indeed, to open a metering machine and install the removable SIM could be a cumbersome task. The SIM should be pre-installed in the machine at manufacturing time. Unfortunately, such pre-installation removes the flexibility of changing mobile operator and subscription that the removable offers. To remedy the situation it is necessary to have an easy installation of the user subscription at the customer site. The challenge is now the multiple alternative solutions to this installation that could have advantages and disadvantages for a certain stakeholder such as operator, SIM manufacturer, terminal manufacturer, etc. In fact, the evolution path of the SIM is quite unclear and confusing.

In this thesis a comprehensive description of the SIM evolution has been given, where three evolution paths have been identified and explained thoroughly. In one path, the SIM will remain removable as it is today while it will be soldered or integrated in the device in the two other solutions. i.e. eUICC and soft SIM. The thesis also provides a security assessment of the eUICC and soft SIM since they have major difference with the current removable SIM.

As future work, it might be relevant to elaborate business model for each SIM evolution path. Thorough studies about the values for the stakeholders, e.g. user, operator, device manufacturer, SIM manufacturer, etc. On the technology side it might be quite interesting to investigate further about the solutions for secure element that is sound to host the SIM or USIM application.

Bibliography

[1] Germann C., (2008) *SECURE SOFT SIM CREDENTIAL TRANSFER*, WIPO Patent No. WO/2008/128874.

[2] Schell S., Narang M., Caballero R., (2011) *WIRELESS NETWORK AUTHENTICATION APPARATUS AND METHODS*, WIPO Patent No. 2011139795.

[3] GSMA, (2011), Embedded SIM Task Force Requirements and Use Cases 1.0 Retrieved from ftp://ftp.3gpp2.org/.

[4] GSMA, (2011), Embedded SIM Task Force Subscription Manager FAQs, Retrieved from ftp://ftp.3gpp2.org/TSGS/Working/_2011/2011-0505-TSG-S+TSG-C_re_eUICC/Embedded

[5] GSMA, (2012), Remote Provisioning Architecture for Embedded UICC, DRAFT 1.34, GSM Association.

[6] GSMA, (2011), Embedded Mobile Whitepaper Embedded Mobile Guidelines Version 2 Retrieved http://www.gsma.com/connectedliving/wp-content/uploads/2012/04/whitepaperembeddedmobileguidelinesv2.pdf

[7] GSMA, (2011), Embedded SIM Task Force Requirements and Use Cases 1.0 Retrieved from ftp://ftp.3gpp2.org/.

[8] Mouly M., Pautet M.B, Foreword B.T., (1992) *The GSM system for mobile communications.* Telecom Publishing, ISBN 0945592154.

[9] Pagliusi P.S., (2002) *A Contemporary Foreword on GSM Security*, Journal of Infrastructure Security, ScienceVolume 2437, pp 129-144.

[10] IUT-T, (2012) *The international identification plan for public networks and subscriptions*, Technical Report, IUT-T Publications Retrieved from http://www.itu.int/rec/T-REC-E.212/en

[11] Meyer U., Wetzel S., (2011) *A man-in-the-middle attack on UMTS*, Proceeding of the 3rd ACM workshop on Wireless security, Oct1-Oct01 Philadelphia , US.

[12] Audestad J.A., (2008) *Technologies and Systems for Access and Transport Networks*, Boston US, Artech House.

[13] Eisl F., (2004) *Smart Card Security Service for an Open Application Environment used in Mobile Phones* (Master Thesis), Department of Information Technology, Lund University, Retrieved from Dissertations and Theses database (http://www.iicm.tugraz.at/)

[14] Markantonakis K., Mayes K.m (2004) *Smart Cards, Tokens, Security and Applications*, New York, Springer, ISBN:9780387721972.

[15] Holcombe B., (Feb. 2004) *Government smart card handbook*, Retrieved from http://www.smartcardalliance.org/resources/pdf/smartcardhandbook.pdf

[16] CDMA Subscriber Identity Module,(n.d.) (2012, July 6), from Wikipedia website, http://en.wikipedia.org/wiki/CDMA_Subscriber_Identity_Module

[17] Jorstad I., Thanh D. V., (2007) *The Mobile Phone as Authentication Token*, Technical Report, Telenor ASA, Norway.

[18] GCMS Reprogrammable SIMs: Technology, Evolution and Implications (2012, Oct 25), from consultantvalueadded website, http://consultantvalueadded.com/

[19] Base Station Subsystem,(n.d.) (2012, November 26), from Wikipedia website, http://en.wikipedia.org/wiki/Base_Station_Subsystem.

[20] ETS, (1994) *European digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (GSM 11.11)*, European Telecommunications Standards Institute, Sophia Antipolis France, Retrieved from http://www.etsi.org/

[21] ETS, (1998) *European Digital cellular telecommunications system (Phase 2+): Specification of the SIM application toolkit for the Subscriber Identity Module-Mobile Equipmen(SIM-ME) interface (GSM 11.14).*, European Telecommunications Standards Institute, Sophia Antipolis France, Retrieved from http://www.etsi.org/

[22] Forsberg D., Moeller W.D., Niemi V., (2011) *LTE security*, New Jersey US, Wiley-Interscience, ISBN:1119957303.

[23] Hallsteinsen, S., (2006) *A study of user authentication using mobile phone*(Master Thesis), Department of Telematics,NTNU, Norway.

[24] Imai H., Rahman M.G., Kobara K., (2006) *Wireless Communications Security*, UK Artech House.

[25] Glendrang M., Hove K., Hvidederg E., (2010) *Decoding GSM*(Master Thesis), Department of Telematics, NTNU,Norway.

[26] Kazi U. K., (2011) *Denial of Service Attacks on UMTS Access*, TTM4137 Wireless Security, Technical Essay, NTNU, Norway.

[27] A5/1,(n.d.) (2012, Dec 15), from Wikipedia website, http://en.wikipedia.org/wiki/A5/1

[28] Starsinic, M. (2010) *System architecture challenges in the home M2M network*, Proceeding of Applications and Technology Conference (LISAT), May7-May9 Texas , US.

[29] What is nano-SIM card,(n.d.) (2012, April), from website, http://3g4g.blogspot.co.uk/2012/04/what-is-nano-sim-card.html

[30] Mobile Virtual Network Operator,(n.d.) (2012, Dec 26), from Wikipedia website, http://en.wikipedia.org/wiki/Mobile_virtual_network_operator

[31] Gemalto,(n.d.) (2012, Dec 28), from Wikipedia website, http://en.wikipedia.org/wiki/Gemalto

[32] Qualcomm,(n.d.) (2012, Dec 30), from Wikipedia website, http://en.wikipedia.org/wiki/Qualcomm

[33] Burr, W. E., Dodson, (2006) *Electronic authentication guideline. NIST special publication.*

[34] Hongsong C., Zhongchuan F., Dongyan Z., (2011) *Security and trust research in M2M system*, Proceeding of Vehicular Electronics and Safety (ICVES), July10-July12 Beijing , China.

[35] Toorani M., Beheshti A., (2008) *Solutions to the GSM Security Weaknesses*, Next Generation Mobile Applications, Services and Technologies. NGMAST'08. The Second International Conference on. IEEE.

[36] Chatrath, v., (2004) *Method and system for associating subscriber identity information*, U.S. Patent Application 10/855,551.

[37] Dierks T. Allen C., (1999), *The TLS Protocol Version 1.0, IETF, RFC 2246*, Retrieved from http://www.ietf.org/rfc/rfc2246.txt

[38] Charlie K. (2005), *Internet key exchange (IKEv2) protocol.*, Retrieved from http://tools.ietf.org/html/rfc4306

[39] Madlmayr, G., Dillinger, O., Langer, J., Schaffer, C., Kantner, C., Scharinger, J (2007, July) *benefit of using SIM application toolkit in the context of near field communication applications*, In Management of Mobile Business, 2007. ICMB 2007. International Conference on the (pp. 5-5).

[40] Cox, Ch., (2009, First Data Corporation) *Trusted Service Manager: The Key to Accelerating Mobile Commerce*, Retrieved from http://www.firstdata.com/downloads/thought-leadership/fd_mobiletsm_whitepaper.pdf

[41] Merrien, L. Mathian, N., Roussel, N., Berard, X., Gachon, D., Girard, P., Proust, P., Vergnes, F., Faria, F., Imoucha, F., Bradley, P.,

(2011) *UICCs EMBEDDED IN TERMINALS OR REMOVABLE THERE FROM*, U.S. Patent Application 13/312,309.