UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

TELECOMMUNICATION ENGINEERING

Nazia Jamil

SECURITY MEASUREMENT FOR LTE/SAE NETWORK DURING SINGLE RADIO VOICE CALL CONTINUITY (SRVCC).

Master´s thesis for the degree of Master of Science in Technology submitted for inspection, Vaasa, 20 May, 2014.

Supervisor Professor	Mohammed Salem Elmusrati
Instructor M. Sc. (Tech.)	Tobias Glocker

ACKNOWLEDEMENT

I owe my deepest gratitude to my supervisor Mohammed Salem Elmusrati and instructor Tobias Glocker who agreed to supervise and instruct me during my thesis work. I would like to share the credit of my work with Tobias Glocker who has taken pain to go through the thesis work and make necessary corrections as and when needed. I am indebted to my faculty for their cooperation and support. My heartfelt thanks to my husband Nadeem and children Eshal & Umer, without their cooperation and sacrifice it would not have been possible. And I am grateful to my siblings, friends and well-wishers for their best wishes and moral support.

TABLE OF CONTENTS **Page**

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
AES	Advance Encryption Standard
AH	Authentication Header
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AMT	Analog Modulation Technology
AMPS	Advance Mobile Phone System
APN	Access Point Name
AS	Access Stratum
ATCF	Access Transfer Control Function
ATGW	Access Transfer Gateway
AuC	Authentication Center
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CA	Certificate Authority
CAP	CAMEL Application Part
CBC	Cipher Block Chaining Mode
CC	Control Channels
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data

CFB	Cipher Feedback Mode
C-I-A	Confidentiality Integrity and Availability
CK	Cipher Key
CN	Core Network
CoMP	Coordinated Multi Point
CRL	Certificate Revocation List
CS	Circuit Switched
CSCF	Call Service Control Functions
CSFB	Circuit Switched Fallback
DES	Data Encryption Standard
DoS	Denial of Service
DDos	Distributed Denial of Service
DS	Data Service
DTM	Data Transfer Mode
E-CSCF	Emergency CSCF
E-UTRAN	Evolved UTRAN
EAP-AKA	Extensible Authentication Protocol-AKA
EARFCN-DL	E-UTRAN's Absolute Radio Frequency Channel Number-DownLink
EATF	Emergency Access Transfer Function
ECB	Electronic Codebook Mode
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EDGE	Enhanced Data Rates for GSM Evolution

EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
EIR	Equipment Identity Register
EIR	Equipment Identity Register
eNB/eNodeB	Evolved Base Station
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
FAP	Femtocell Access Point
FIFO	First In First Out
GEA	GPRS Encryption Algorithm
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSMA	GSM Association
GTP	GPRS Tunneling Protocol
HE	Home Environment
HeNB/HeNodeB	Home eNB
HLR	Home Location Register
HMAC	Hashing for Message Authentication Code

HSCSD	High-Speed Circuit-Switch Data
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
IAA	Identify Authenticate Authorize
IK	Integrety Key
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity Module
IMT-MC	International Mobile Telecommunications Multi-Carrier
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISIM	IMS Subscriber Identity Module
ISMI	International Mobile Subscriber Identity
ISUP	ISDN User Part
IWF	Inter Working Function
KAC	Key Administration Center
KDF	Key Derivation Function
KSI	Key Set Identifier
LSB	Least Significant Bits
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Message Authentication Code

MAP	Mobile Application Part
MAPsec	MAP Security
ME	Mobile Equipment
MGCF	Media Gateway Control Function
MGW	Media Gateway
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
MMS	Multimedia Message Service
MoTTPS	Management of Trusted Third Party Services.
MS	Mobile Station
MSC	Mobile Services Switching Center
MTC	Machine Type Communication
NAS	Non Access Stratum
NAT	Network Address Translation
NCC	Next hop ChainingCounter
NDS	Network Domain Security
NGMN	Next Generation Mobile Network
NH	Next Hop
NIST	National Institute of Standards & Technology (US)
NMT	Nordic Mobile Telephone
NSS	Network Sub System
OFB	Output Feedback Mode
P-CSCF	Proxies CSCF
PCI	Physical Cell Identity

PCRF	Policy Control and Charging Rules Function
PDN	Packet Data Network
PGP	Pretty Good Privacy
P-GW	Packet Data Network Gateway
P-TMSI	Packet Temporary Mobile Subscriber Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRF	Pseudo Random Function
PS	Packet Switched
PSHO	Packet Switched HandOver
PSTN	Public Switched Telephone Network
QCI	Quality of Service Class Indicator
QoS	Quality of Service
RA	Reasonable Assurance
RA	Registration Authority
RAN	Radio Access Network
RF	Radio Frequencies
RAT	Radio Access Technology
RC	Radio Channels
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control
S-CSCF	Serving CSCF
S/MIME	Secure/Multipurpose Internet Mail Extensions

SAGE	Security Algorithms Group of Experts
SA	Security Association
SAE	System Architecture Evolution
SCC AS	Services Centralization and Continuity Application Server
SEG	Security Gateway
SIP	Session Initiation Protocol
SGSN	GPRS Support Node
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SIM	Subscriber Identity Module
SMS	Short Messaging Service
SN	Serving Network
SPIT	Spam over Internet Telephony
STN-SR	Session Transfer Number for SRVCC
VoLGA	Voice over LTE via GAN
VoLTE	Voice Over LTE
SRVCC	Single Radio Voice Call Continuity
SSH	Secure Shell
SSL	Secure Socket Layer
SVLTE	Simultaneous Voice and LTE
TCH	Traffic Channel
TLLI	Temporary Logical Link Identifier
TMSI	Temporary Mobile Subscriber Itedentifier
UE	User Equipment

UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
UTRA	Universal Terrestrial Radio Access
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register
VoLTE	Voice Over LTE
VPLMN	Visited Public Land Mobile Network
vSRVCC	Single Radio Video Call Continuity
WCDMA	Wideband Code Division Multiple Access
Wi-Fi	Wireless Fidelity (IEEE 802.11b wireless network)
WiMAX	Worldwide Interoperability for Microwave Access (IEEE 802.16 wireless broadband standard)
WWWW	Wireless World Wide Web

UNIVERSITY OF VAASA	
Faculty of Technology	
Author:	Nazia Jamil
Topic of the Thesis:	Security Measurement for LTE/SAE During Single Radio Voice Call Continuity (SRVCC).
Supervisor:	Professor Mohammed Salem Elmusrati
Instructor:	Tobias Glocker
Degree:	Master of Science in Technology
Department:	Department of Computer Science
Degree Programme:	Degree Programme in Information Technology
Major of Subject:	Telecommunication Engineering
Year of Entering the University:	2006
Year of Completing the Thesis:	2014 **Pages:** 120

ABSTRACT:

Voice has significant place in mobile communication networks. Though data applications have extensively gained in importance over the years but voice is still a major source of revenue for mobile operators. It is obvious that voice will remain an important application even in the era of *Long Term Evolution* (LTE). Basically LTE is an all-IP data-only transport technology using packet switching. Therefore, it introduces challenges to satisfy quality of service expectations for circuit-switched mobile telephony and SMS for LTE capable smartphones, while being served on the LTE network. Since 2013, mobile operators have been busy deploying *Voice Over LTE* (VoLTE). They are relying on a VoLTE technology called *Single Radio Voice Call Continuity* (SRVCC) for seamless handover between packet-switch domain to circuit-switch domain or vice versa. The aim of thesis is to review and identify the security measurement during SRVCC and verify test data for ciphering and integrity algorithm.

KEYWORDS: 3GPP, GSMA, LTE/SAE, UMTS, GSM, E-UTRAN, UTRAN, GREAN, CS, PS, Handover, IMS, VoLTE, SRVCC, IRATs, VCC, STN-SR, DTM, PSHO, Kasumi, Snow 3G, ZUC, AES, lu, Integrity and Ciphering algorithms.

1. INTRODUCTION

In today’s cellular phones and by extension cellular networks have become an important part of everyday life. They are used for both personal and business dealings and over the years they have developed into all in one device that are used for everything from basic voice communication to video sharing and surfing the web. Consequently the communication technologies behind these cellular networks have also evolved to handle the extended range of data types and requirement for additional bandwidth. As people have begun to use their mobile phones for more personal aspects of their lives, the need has also increased to make the service secure and reliable.

Mobile networks are more and more used to transmit also mission critical data in everyday business life. The operation scenarios are varied. It starts from simple reading of e-mail communication or synchronization of contacts and appointments while external working and ends with direct access to business intern applications for controlling production processes.

Nevertheless data transmission via mobile networks is often integrated in business processes,without knowing the therewith associated applied threats. Consequently, suitable measures that make data transmission secure are not applied at all or not in an appropriate way.

The best way to appreciate security is by looking at vulnerabilities, risks, threats and attack to a mobile communications system. At any given moment, anybody could eavesdrop into your conversation. Your bank account information, daily schedule, and any other information you may disclose on the phone would be at risk.

Objective to do this thesis is to take a look at security measurements in cellular especially mobile network in general and in SRVCC procedure particularly along with test data sets verification against UIA, UEA, EIA and EIA algorithms for UMTS and LTE network.

The thesis consists of five chapters. In the second chapter, introduction of network is presented, to give a brief idea of architecture, operation and evolution of cellular network. And in the third chapter concrete idea of information and communication security and security related algorithms, functions, attacks, risk, and protocols is presented. Forth chapter is about evolution of security mechanism in mobile network including GSM, GPRS, UMTS and LTE. This chapter helps to identify possible vulnerabilities, risks, threats, attacks, security architecture, security mechanism and cryptographic algorithms for a cellular network from generation to generation in general (see **Figure 1**). Fifth chapter is about to identify the security measurement of *voice call continuity* (VCC) during *Interworking Radio Access Technologyies* (IRATs). Security keys derivation during SRVCC triggered handover, exchange of security parameters during the E-UTRAN and UTRAN/GERAN SRVCC triggerd mobility and verification of test data sets for integrity and ciphering provided by 3GPP, ETSI/SAGE and GSMA are presented in this chapter. Last chapter comprises of conclusion and future work proposals.

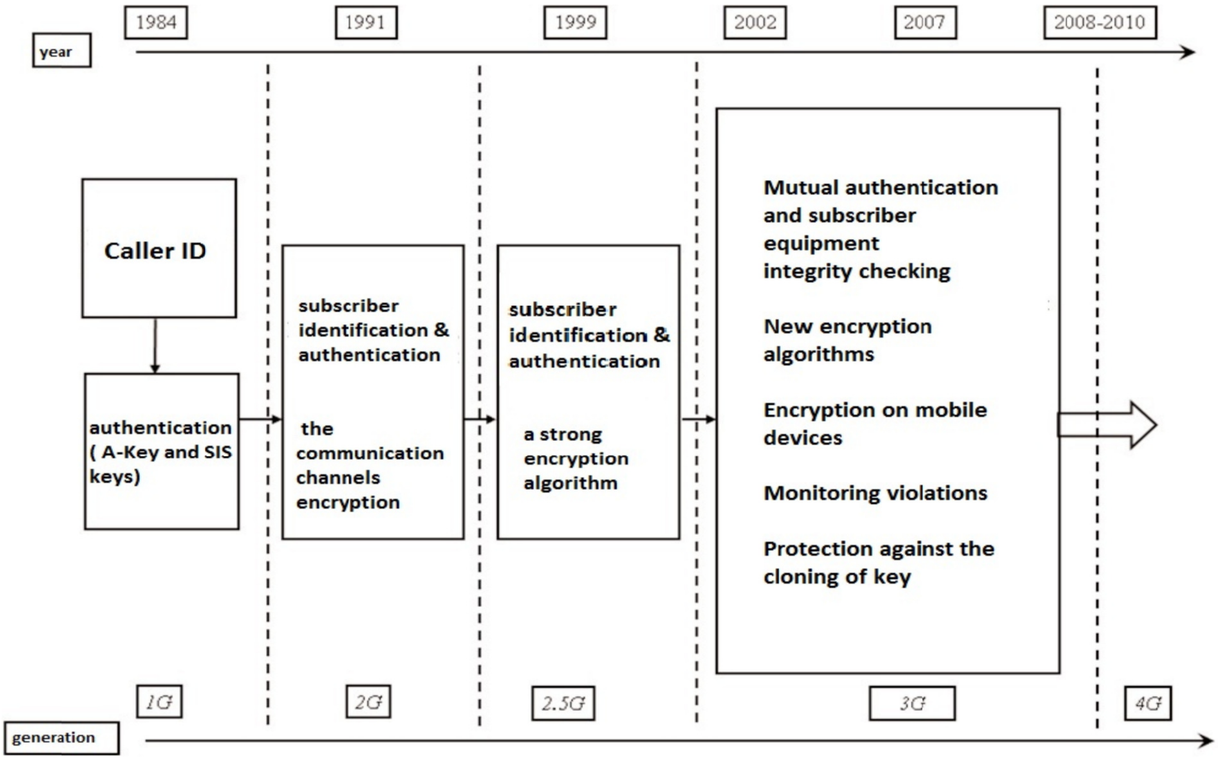

year
1984
1991
1999
2002
2007
2008-2010
Caller ID
authentication (A-Key and SIS keys)
subscriber identification & authentication
the communication channels encryption
subscriber identification & authentication
a strong encryption algorithm
Mutual authentication and subscriber equipment integrity checking
New encryption algorithms
Encryption on mobile devices
Monitoring violations
Protection against the cloning of key
1G
2G
2.5G
3G
4G
generation

Figure 1. Evolution of Security Mechanisms (Mazurkevich & Orlov 2011).

2. CELLULAR COMMUNICATION

Cellular communication has become a significant part of our daily life. We can’t imagine our life without cellular communication including voice communication, video conversation, monetary transactions, and text messaging etc. Cellular mobile communication system has been categorized into five generations. So for better understanding here is brief background of cellular technology and generations of mobile networks.

2.1. Cellular Technology

Cellular network is network made up of a number of cells, uses a complex two-way radio system between the mobile unit and the wireless network. It uses *radio frequencies* also known as *radio channels* over and over again through a market with minimal interference, to serve a large number of simultaneous conversation. This idea is the central principle to cellular design and known as *frequency reuse*.

Cell: Geographical areas covered by cellular radio antennas are called cells. A cell corresponds to the covering area of one transmitter or a small collection of transmitters. The size of a cell is determined by the transmitter's power. The main idea of cellular systems is the use of low power transmitters to achieve the efficient reuse of the frequencies. A cell site lies at the edges of the several cells; middle circle in the **Figure 2** shows the cell site.

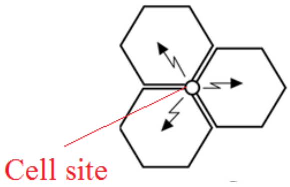


Figure 2. Cell Site (Nilanka 2011).

Cluster: Cluster is a group of cells and very important part of cellular network (see **Figure 3**). The cluster can be repeated *continuously* within the covering area of an operator. Generally a cluster contains *4, 7, 12 or 21 cells* and the number of cells in each cluster is very important. The number of cells per cluster is inversely proportional to the number of channels per cell.

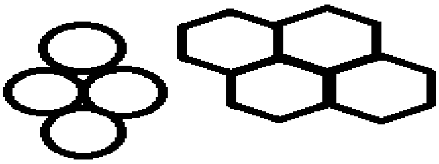


Figure 3. Cluster (Nilanka 2011).

Type of Cells: Different types of cells are used according to varied density of population in a country. Large cells for remote and sparsely populated areas are covered by macrocells. Densely populated areas are covered by micro cells. Selective cells are used when *cell with a particular shape and coverage are needed.* A good example of selective cells is the cells that may be located at the entrances of tunnels where, coverage of 360 degrees is not required. In this case, a selective cell with coverage of 120 degrees is used. And umbrella cells cover few *microcells*; for instance when *the speed of the mobile is too high, the mobile is handed off to the umbrella cell*, and the mobile will then stay longer in this cell. (Pagtzis 1999.)

2.2. Channel

Mobile phones and transmitter communicate with each other via *dedicated paired frequencies* called *channels*. Control channel and traffic channel are two main channels. Control channels establish connection between mobile unit and nearest base station and take care of setting up and maintain calls. And traffic channels carry voice or data connection between users.

2.3. Operation of Cellular System

This section will give the brief introduction of important component of cellular system: The *Base Station* (BS) is the interface between wireless phones and traditional wired phones. It’s what allows you to use your cell phone to call your home phone. It is located at centre of each cell and it comprises of antenna, controller and transceivers. *Base Transceiver Station* (BTS) is the radio transmission part of the base station system. *Base Station Controller* (BSC) is the control part of BSC performs the switching function in BSC.

Mobile Services Switching Center (MSC) connects calls between mobile units and from mobile to fixed telecommunications network, assigns voice channel, performs handoffs and monitors calls (for billing). It obtains all the data for processing subscriber call requests from 3 types of databases (HLR, VLR and AUC). *Visitor Location Register* (VLR) stores all related information of mobile subscribers those who enter into its coverage area. *Home Location Register* (HLR) stores the related data of all existing mobile subscribers controlled by the same HLR and one HLR can control several mobile switching areas.

2.4. Generation of Cellular Network

Cellular networks have been around since 1980s and it is getting more and more subscriber over the time period. **Figure 4** depicts the evolution of cellular network generation by generation along with modulation techniques.

1G (1980s)

First generation networks were able to transmit voice at the speed of 9.6 kbps. *Advance Mobile Phone System* (AMPS) and *Nordic Mobile Telephone* (NMT) were the known cellular networks in USA and Europe respectively and were using *Analog Modulation Technology* (AMT) for data transmission. There was no cryptography implemented and sound quality was also very poor. Besides, use of the spectrum was inefficient because of analog technology. (Gardezi 2006; Nilanka 2011.)

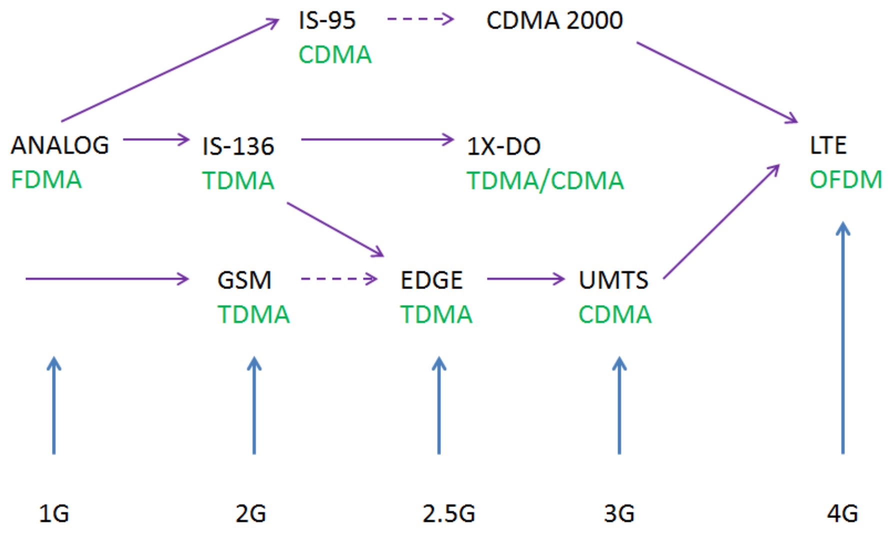


Figure 4. Evolution of Cellular Networks.

2G & 2.5G (1990s)

Second generation networks are far much better then 1G but they were also only using voice communication and known as Global System for Mobile Communications (GSM). GSM is the most widely adopted technology by all over the world and it uses *Gaussian Minimum Shift Keying* (GMSK) modulation. 2.5G is a transition step between 2G and 3G and is also known as *data services over 2G*.

Some famous data services which are part of the 2.5G extensions are following:

Short Messaging Services (SMS) transfer short messages between cell phones, but if message is large then it chops the message into several short messages and then send multiple messages.

High-Speed Circuit-Switch Data (HSCSD) was the first technique to provide data at high speed over GSM with 115 kbps speed, but it does not support large bursts of data.

General Packet Radio Service (GPRS) is more popular technique and of course supports large bursts of data transfer. The prominent features of this technique are *Service GPRS Support Node* (SGSN) for security, mobility and control mechanisms, and *Gateway GPRS Support Node* (GGSN) for connectivity to external packet switch network.

Enhanced Data Rates for *GSM Evolution* (EDGE): This uses 8-PSK modulation. It provides up to 348 kbps speed in combination of GPRS.

Cellular Digital Packet Data (CDPD): This is packet base data service and able to identify idle voice channels, and utilizes those idle channels for transferring data traffic without interrupting voice communication.

CDMA-1 is also known as IS-95a and was initial 2G technique used by USA. It allows using the entire spectrum by user and supports more users than TDMA and GSM. CDMA-2 provides 115.2 kbps speed. (Gardezi 2006; Nilanka 2011.)

3G (2000s)

Third generation is known as *Universal Mobile telecommunication Systems* (UMTS) in Europe and as a CDMA 2000 in U.S.A. It is based on *Universal Terrestrial Radio Access* (UTRA) radio interface and extended GSM/GPRS network. 3G is a family of standards which can all work together and WCDMA is the air-interface for the UMTS. The second *Interface IMT Multicarrier* (IMT-MC) is backward compatible with IS-95, and provides seamless transitions to 3G. It comprises of BS (Base Station) or node B, RNC (Radio Network Controller), along with *Wideband CDMA Mobile Switching Centre* (WMSC) and SGSN/GGSN. UMTS is broadband and offers packet-based transmission of text, digitized voice, video, and multimedia up to or higher than 2 mbps. The first commercial 3G network was launched by NTT Do Co Mo in Japan branded FOMA, based on W-CDMA technology in 2001.

4G (2012)

The fourth generation is 3GPP's Long Term Evolution(LTE). Enhanced Multiple-Input Multiple-Output (MIMO) channel transmission techniques and extensive coordination among multiple cell sites called Coordinated Multipoint (CoMP) transmission/reception are key techniques for LTE. 4G offers high-quality service and fast data transfer rates. It needs a data speed transfer rate of 100 mbps while a user moves at high speed, and a 1Gbps data rate in a fixed position. It also needs to share the network resources to support more simultaneous connections on the cell. Phones on a 4G network also need to use Internet Protocol (IP) technology for data transfers through packets.

5G (2020)

5G is still in theory currently and has not been implemented yet. However, 5G is complete wireless communication with almost no limitations, thus, can be called REAL wireless world, when implemented it would have incredible transmission speed, and would be capable of supporting *wireless world wide web* (WWWW). It would reach 25Mbps connectivity speed, while uploading and downloading speed up to 1Gbps.

3. BASIC SECURITY CONCEPTS

Basic concept of security, introduction of information and communication security, and cryptography is being discussed in this chapter. This chapter will give the road map of security and its related algorithms, functions, attacks, risks, and protocols.

3.1. Security

Basic definition of the security is "freedom from fear, anxiety, danger or doubt and having a state of safety or certainty". But it is bit relative measure and we can say that no system is absolutely secure system we only can try to take all possible measures to protect a system. Security systems only offer a set of steps for *protection* (safety) over targeted *resources* (assets) against the mentioned or identified *dangers* (threat).

Security can be grouped as security mechanism, security service and security attack. Where security mechanism is designed to detect, prevent or recover a system from attack(s) is known as security mechanism. Security serviceenhances the security of the data processing and the information transfers of an organization. "The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service" (Stallings 2010). And security attack is defined as "any action that compromises the security of information owned by an organization" (Stallings 2010).

3.2. Information Security

Information security is to protect the information system and data from unauthorized access, use, disclosure, disruption, modification, tampering or destruction. Confidentiality, integrity and availability are there objectives of information security.

Confidentiality means "information that should stay secrete stays secrete and only authorized person may access it" (Fundamental Security Concept 2013). Cryptography and access control are main mechanism of protection confidentiality in the information systems. And malware, intruders, social engineering, insecure networks, and poorly administrated systems are examples of threats to confidentiality.

Integrity deals with the trustworthiness, origin, completeness, and correctness of information. It prevents information from unauthorized or improper modifications. It not only deals with integrity of information itself but also with the integrity of origin.

Integrity protection mechanism may be grouped in two broad categories: preventive mechanisms and detective mechanisms. *Preventive mechanism* is such as access controls that prevent unauthorized modification of information. *Detective mechanisms* detect unauthorized modifications when preventive mechanisms became failure.

Availability is as important and necessary as confidentiality and integrity are. It tells that, who needs confidentiality and integrity if the authorized users cannot access and use the information? Who needs sophisticated encryption and access controls if the protected information is not accessible for authorized users and when they need it? *Denial of service* (DoS) attacks belongs to this category.

Confidentiality, integrity, and availability (*C-I-A*) triad have some of the main controls aimed at protecting such as identification, authentication, and authorization process and methods.

Identification is the very first step of *identify-authenticate-authorize* sequence that is performed everyday by humans and computers when access to information or information processing resources is required. While particulars of identification system differ depending upon who or what is being identified, some intrinsic properties of identification apply regardless of these particulars. These three are intrinsic properties are scope, locality, and uniqueness of IDs.

“For information security, unique names are required and, depending on their scope, they must be locally unique and possibly globally unique so that access control may be enforced and accountability established” (Fundamental Security Concept 2013).

Authentication is a verification of the identity declared at the stage of identification. What you know, what you have, or what you are; are three methods of authentication.

To obtain reasonable assurance for declared identity belong to the party in communication is aim of authenticity. It is important to note that *reasonable assurance* may mean different degrees of assurance, depending on the particular environment and application, and therefore may require different approaches to authentication" (Fundamental Security Concept 2013).

Authorization is next step to identification and authentication; users are assigned a set of authorization (e.g. rights, privileges, or permissions) that defines what they can do on the system. These authorizations are usually defined by the system or security administrators.

Accountability "refers to possibility of tracing actions and events back in time to the users, systems, or process that performed then, to establish responsibility for action or omission" (Fundamental Security Concept 2013). It can be provided by logs and audit trials in context of information system.

Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. In international ISO 14516: 2002 (*guidelines for usage and management of trusted third party services)*: approval, sending, origin, submission, transport, receipt, knowledge and delivery aretypes of non-repudiation services.

3.3. Design Principles of Security

Different principles ofsecurity design can be seen in **Table 1.** Followings are steps/ principles to design a secure information or communication system.

Table 1. Design Principle of Security.

Threat analysis	To list down all possible threats against the system, regardless of difficulty and cost measurements.
Risk analysis	To Estimate the probability of various attacks and the potential gain

	for the attackers and/or damage to the attacked side cause by them.
Requirements capture	Depending on the earlier phases, it is now decided what kind of protection is required for the system.
Designs Phase	"The actual protection mechanisms are designed in order to meet the requirements. Existing building blocks, such as security protocols or primitives, are identified. Possibly new mechanisms are created, and security architecture is built. This is also possible that not all requirements can be met, so we have to take constraints into account. This may cause a need to re-visit earlier phases, especially risk analysis" (Forsberg, Horn, Moeller & Niemi 2010: 11).
Security Analysis	It can be done by using automation verification tools and by using creative method we can identify holes in the security system.
Reaction Phase	This is not possible to plan everything beforehand, so it is very important to design a flexible mechanism. In case of unexpected reaction a mechanism should be capable of allowing enhancement. It is always useful to have reasonable amount of safety margin in the mechanism. "These margins tend to be useful in cases where new attack methodologies appear faster than expected. (Forsberg et al. 2010: 11.)

3.4. Security Vulnerability, Threat Risk & Attack

To secure the system we should identify the vulnerabilities, threats and attacks towards the system. Vulnerability is any procedural weakness that may allow an attacker to enter and exploit the resources with unauthorized access. In simple words it is absence of weakness of safeguard.

Threat is any potential danger towards the system or networks. It is a possibility that someone could identify and exploit the vulnerability. The entity that takes the advantage of vulnerability is known as threat agent. And risk is frequency of threat agent taking advantage of vulnerability. Risk can be reduced by reducing vulnerability and/or threats.

3.4.1. Threat and Risk Assessment

Along with these above mentioned steps, the threat and risk assessment should be taken into account. The objective of a threat and risk assessment is to provide services or recommendations, for maximizing the protection of confidentiality, integrity and availability along with functionality and usability.

Egners, Rey, Schmidt, Schneider & Wessel (2012: 14) have mentioned, that a *threat* is "a potential cause of an incident that may result in harm to a system or organization" and a *vulnerability* as "a weakness of an asset or group of assets that can be exploited by one or more threats". While according to them a threat can be categorized with respect to availability, confidentiality and integrity and those could be loss of availability, confidentiality, integrity and control. In mobile network the most significant threat is theft of service which is in result of integrity or confidentiality breaking.

Loss of availability is comprises of flooding an interface and crashing a network through protocols or flaw of application implementation. Loss of confidentiality is comprises of eavesdropping and unauthorized access to sensitive data on a network element through leakage. Loss of integrity is composition of traffic modification and data insertion. Loss of control is compromise or/and abuse of network elements. It could be happened by protocols/applications implementation vulnerability, by management interface or by insider malicious. And theft of service is defined as: attacker exploits a flaw such as the authentication and authorization mechanisms to use services without being charged. (Egners et al. 2012: 20-22.)

“The potential or possibility of compromise, loss, injury or other adverse consequence” is called Risk. It can be formulized in the simplest way as following:

$$\text{The Risk (to an Asset)} = \text{Threat x Vulnerability x Impact/Consequence} \qquad (\mathbf{1})$$

(Langham 2013.)

From equation (**1**) it can be seen that Risk is overlapping of threat and vulnerability. We are at a risk when our systems have a vulnerability which allows the threat to attack. Risk management is the process of identifying, analyzing, evaluating and reducing the risks of a system and it is to weigh and make decisions about acceptable risk.

3.4.2. Attack

Basic definition of attack can be: “any action that compromises the security of information”. In other words an attack can be defined as “any malicious or accident disruption in the confidentiality, integrity or availability of information or network resources” (UNT 2003). Attacks can be grouped in four basic categories: *access, modification, denial of service* and *repudiation* and those can come from many places, electronics, physical or human. **Table 2** shows the matrix of attacks where: access attacks are possible for confidentiality and accountability, modification attack is possible at integrity and accountability, DoS attack is possible at only availability and repudiation attack is same as modification.

Table 2. Information Security Matrix (UNT 2003).

	Security Objectives			
Attack Types	Confidentiality	Integrity	Availability	Accountability
Access	X			X
Modification		X		X
DoS			X	
Repudiation		X		X

3.5. Basic Concept of Cryptography

Cryptology is *an ancient art and science of secrete (crypto) writing (graphy).* Secrete writing including the principles and methods of transforming an intelligible message into unintelligible, and then retransforming that message back to its original form. It is tremendous tool to provide the basis of many security mechanisms, but it is not the solution of all security problems and not reliable unless implemented and used properly.

Security objectives such as *authentication*, *privacy/confidentiality*, *Integrity*, *Non-repudiation* can be obtained by applying cryptology techniques. Cryptology comprises of crypto-graphy which is practice of using cryptosystems to maintain the confidentiality or designing system by using cryptologic techniques and crypto-analysis which is a study of breaking cryptosystem or try to identify weakness in cryptosystems and it contributes indirectly to achieve a better security level. Key words for cryptography are defined in **Table 3**.

Table 3. Key Words for Cryptography.

Plaintext (P)	The original intelligible or readable message or data that is fed into the cipher algorithm as an input.
Cipher	An algorithm, used for transforming the intelligible message into one that is unintelligible by transposition and/or substitution method.
Key (K)	Critical information used by the cipher, known only to the sender and receiver.
Ciphertext (C)	Transformed or scrambled unintelligible message produced as an output of encryption. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
Encipher (E)	The process of converting plaintext into ciphertext by using

	cipher and key.
Decipher (D)	Reverse process of encoding, here ciphertext is converted back to plaintext by using cipher and key.
Encryption algorithm	A mathematical function $C = E(P, Ke)$ **(2)** Where C is ciphertext, E is encipher, P is plain text and Ke is encryption key. (Yang 2008.)
Decryption algorithm	Reverse mathematical function with the matching key. $P = D(C, Kd)$ **(3)** Where P is plaintext, D is decipher, C is ciphertext and K_d is encryption key*. (Yang 2008.)
Cryptanalysis (attacker, intruder)	The study of principle and methods of transforming an unintelligible message back into an intelligible message without knowing of the key.

Cryptosystem can be categorized as *conventional* and *modern cryptography*. In conventional cryptography the encryption algorithms are designed to be rather complex and difficult to guess. But in modern technique an encryption algorithms are made public but keys are kept secret. The strength of algorithm depends upon how difficult of determining K_d.

Symmetric encryption uses a single secret key between sender and intend receiver.

$$D\ (E\ (p, k), k\ ) = p \qquad \textbf{(4)}$$

Where D is deciphering, E is enciphering, p is plaintext and k is key.

(Forsberg et al. 2010: 14.)

Asymmetric encryption uses two keys one is public key and another is private key. The public key is available for everyone, but the private key is only known by the owner. When the message is encrypted with the public key, only the corresponding private key can decrypt the message.

$$D\ (E\ (p, k1), k2\ )\ =\ p \qquad (\mathbf{5})$$

Where D is deciphering, E is enciphering, p is plaintext and k1&k2are keys (these are not identical, and k_2 cannot be easily derived from k_1. (Forsberg et al. 2010: 14.)

3.6. Symmetric or Conventional Cryptography

Conventional or symmetric encryption methods are divided into two main categories: *block* and *stream* cipher.

3.6.1. Stream Cipher

This algorithm encrypts bits individually and can be achieved by adding a bit from a key stream to a plaintext bit. There are *synchronous* stream ciphers where the key stream depends only on the key, and *asynchronous* where the key stream depends on the key and ciphertext both. In **Figure 5**, the gray thin line shows, the stream cipher is an asynchronous one but practical stream ciphers are synchronous. Stream ciphers are particularly related to the applications with little computational resources because they tend to be small and fast, e.g., for cell phones or other small embedded devices. A very significant example for a stream cipher is the A5/1 cipher, which is part of the GSM mobile phone standard and is used for voice encryption. And sometimes Stream cipher is also used for encrypting Internet traffic, especially the RC4. (Paar & Pelzl 2010: 30-31.)

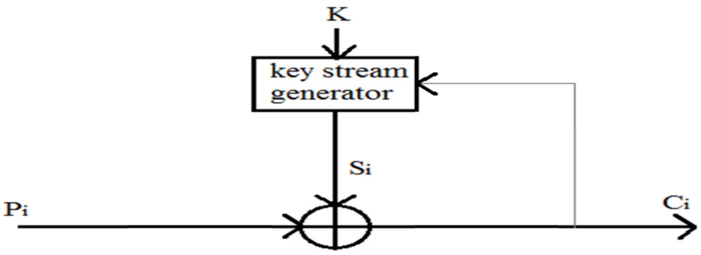


Figure 5. Synchronous and Asynchronous Stream Cipher (Paar & Pelzl 2010: 30).

3.6.2. Block Cipher

Block cipher is an encryption algorithm that takes a fixed length (n bits) block of message (*plaintext*) and a *key* (k bits), and produces a block of *ciphertext* of the same length (n bits) as the plaintext (see **Figure 6**). This key can be reused for different plaintext blocks.

$$c = E(p,k);\ p = D(c,k) = D(E(p,k),k) \qquad \textbf{(6)}$$

Where c is ciphertext, E is enciphering, p is plaintext, k is a key and D is deciphering.

(Forsberg et al. 2010: 16.)

The dominate block cipher in the past was *Data Encryption Standard* (DES) with 64 bits message and 56 bits key length. A newer common use ciphers are *Advance Encryption Standard* (AES) with 128 bits block and 128 bits (minimum) key length.

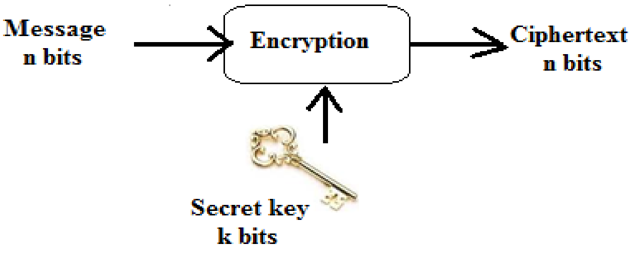


Figure 6. Block Cipher.

Iterative Cipher: Generally block cipher becomes stronger when it is iterated several times. In the design of block cipher, iteration is used inside the block cipher. These iterations s are called *rounds*. An iterative cipher starts with simple but useful function and iterates for many rounds until it is *secured*. Security can be increased by adding the rounds but it will also cause to increase the processing time.

Confusion and Diffusion: Shannon in 1948 introduced two concepts as basic building blocks for designing cryptographic systems confusion which is the “relationship between *plaintext* bit and *ciphertext* bit (should be as complex and involved as possible)” (Forsberg et al. 2010: 17). And diffusion means each *plaintext* bit and each *encryption key* bit should affect each *ciphertext* bit.

Modes of Operation

Block cipher encrypt fixed-sized block e.g. DES encrypts 64-bits blocks, but what happens when plaintext is longer than the size of a cipher block or plaintext is not a multiple of cipher block size? to take care of these problems, NIST has defined several methods called “modes of operation”. There are five modes of operation:

Electronic Code Book (ECB): In this mode, each plaintext block is encrypted independently without any input from other block. From equation (**7**) and the **Figure 7,** “each ciphertext block is obtained by applying the DES encryption process to the current plaintext block directly. So the current ciphertext block has no dependency on any previous plaintext blocks” (Yang 2014).

$$Ci = DES\,(K, Pi) \qquad (\mathbf{7})$$

Where C is ciphertext, DES is Data Encryption Standard algorithm, K is key, P is plaintext and iisa counter. (Yang 2008.)

Encryption and decryption could be parallel done could be advantage of this mode.

Two blocks of with identical plaintext produces identical ciphertext and bit error in one block affects the whole block and plaintext patterns are still visible after encryption done can be considered as disadvantage of this mode. (Syben 2011.)

Cipher Block Chaining (CBC): From equation (**8**), each block of plaintext is XORed with the previous ciphertext block before being encrypted to generate the current ciphertext block. And also note that for the first block, the Initial Vector (IV) is used as the previous ciphertext block.

$$Ci = DES(K, Pi \oplus Ci - 1);\ C0 = IV \qquad (\mathbf{8})$$

Where C, DES, P is same as in equation (**7**)**.** While C_0 is initial value and IV is initial vector. (Yang 2008.)

Decryption could be parallel done and plaintext patterns are blurred are advantages of this mode. Encryption has to be done sequentially and bit error in one block affects two blocks are disadvantages of this mode. (Syben 2011.)

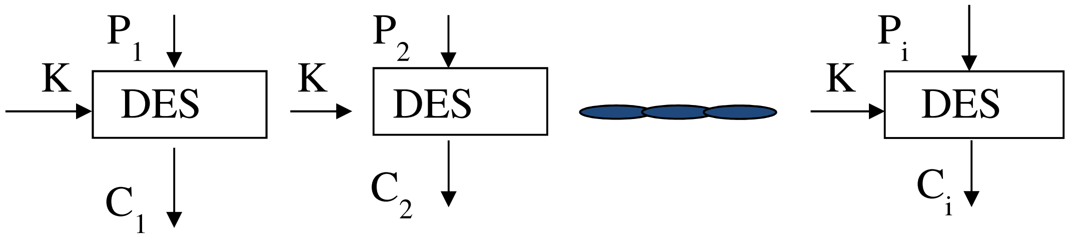


Figure 7. Electronic Code Book (ECB) Mode (Yang 2008).

Output feedback (OFB): In this mode, each plaintext block is XORed with the current output block to be the ciphertext block. The current output block is the encrypted version of the previous output block. Key stream can be pre-computed, no padding is required and bit error only affect one bit are advantages of this mode. Key-stream computation cannot be done in parallel, reusing of key an initialization vector is at risk and bit-flipping attacks are convenient are disadvantages of this mode. (Syben 2011.)

Cipher feedback mode (CFB): In this mode, each plaintext block is XORed with the encrypted version of the ciphertext of the previous block to be the ciphertext block. Decryption could be done in parallel and plaintext patterns are blurred are advantages of this mode. No padding is required, bit error only affects one bit, and decryption can be parallelized are disadvantages of this mode. (Syben 2011.)

Counter mode (CTR): This mode uses cipher block as pseudorandom *bit* generator and encrypts a known string of numbers in ECB mode, producing a string of output blocks DES (K, Ii) (see equation (**9**)).

$$Ci = Pi \oplus DES\ (K, Ii) \qquad (\mathbf{9})$$

Where I is random bit and iis a counter. (Yang 2008.)

Encryption/decryption of each block could be parallelized, no padding is required, and keystream can be pre-computed and can be done in parallel are advantages of this mode. Bit-flipping attacks are convenient, reusing of key and nonce/counter is at risk are disadvantages of this mode. (Syben 2011.)

3.6.3. Comparison of Symmetric Encryption Algorithms

Table 4 is showing the comparison of different symmetric encryption algorithm with key lengths vs strength.

Table 4. Symmetric Encryption Algorithm (Yang 2008).

Algorithm	Strength	Key Length
3DES	Strong	64, 112, 128

Advanced Encryption Standard (AES)	Strong	128, 192, 256
International Data Encryption Algorithm (IDEA)	Strong	64,128
Blowfish	Weak	32, 448
RC4	Weak	
RC5	Strong	32, 64, 128

3.6.4. Problems with Symmetric Encryption

"A single key must be shared in pairs of each sender and receiver. In a distributed environment with large numbers of combination pairs involved in many-to-one communication topology, it is difficult for the one recipient to keep so many keys in order to support all communication" (Yang 2008).

Key management: setting up and acquisition of the secret key. The integrity of data could be compromised when the receiver cannot get assurance that the message has not been modified before receipt. "It is possible for the sender to repudiate the message because there are no mechanisms for the receiver to make sure that the message has been sent by the claimed sender" (Yang 2008).

3.7. Modern or Asymmetric Cryptography

Asymmetric cryptography is also known as *public-key cryptography*. It was invented in 1976 by Whitfield Diffie and Martin Hellman for this reason; sometime it is called *Diffie-Hellman encryption.* It relies on the existence of a computational primitive called *trapdoor or one-way function*. Such a function is easy to perform in one direction, but difficult or impossible to reverse. From **Figure 8**, we can see that sender takes receiver's public key and uses it to encrypt the plaintext. Only Receiver can then decrypt the encoded text, because he is the only one who knows the corresponding private key. Asymmetric ciphers are quite slow then the symmetric ones, which is why asymmetric ciphers are used only to securely distribute the key.

Few famous asymmetric encryption algorithms are *RSA*, D*igital Signature Algorithm* (DSA), *Diffie-Hellman Key Exchange*, *ElGamal*, *Elliptic Curve Cryptography* (ECC), and *Elliptic Curve Digital Signature Algorithm* (ECDSA).

This cryptography is very useful with many-to-many relationship because of easier key management for large systems. The possibility to use digital signatures leads to the possibility for non-repudiation. And also it is useful to solve the scalability problem, because everyone will need only one public key and one private key to communicate with other people.

It has disadvantages such as it is slower than secret key cryptography (or symmetric cryptography) methods, due to high computational requirements. It uses a fixed buffer size, depending on particular and small data amounts, which may only be encrypted and not chained in streams. And it is more robust and less liable to third party security breach attempts because a broad range of possible encryption keys are used.

3.7.1. Digital Signature

The most significant benefit of public key cryptography is that, it provides a method for implementing *digital signatures*. "Digital signatures enable the recipient of information to verify the *authenticity* of *the information's origin* and also verify that the information is intact. Thus, public key digital signatures provide *authentication* and data *integrity*. A digital signature also provides *non*-repudiation" (Zimmermann 2000: 19-20).

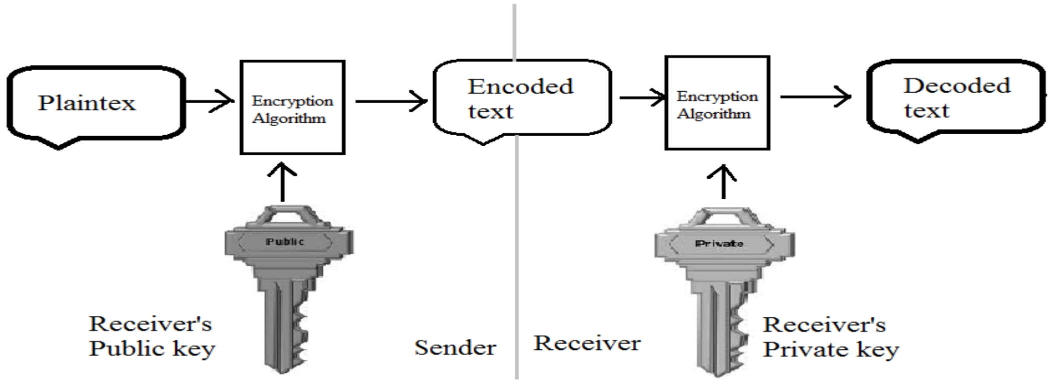


Figure 8. Asymmetric or Public-key Cryptography.

3.7.2. Public Key Infrastructure (PKI)

A PKI is a combination of software and procedures providing a means for managing keys and certificates, it allows internet or other public network's users to have a secure communication, data exchange and money transaction. PKI is done by public and private key algorithm in which key pairs are provided by a *Certificate Authority* (CA). The private key is given to the person who requests for it and the public key is made public in a directory for users. No one can ever find out what someone's private key is and it is never published on the internet. The private key is used for proving user identity and encrypting the *digital certificate*. The digital certificate is decrypted by the public key, which is used by the message receiver.

The registration process for a digital certificate begins with a *Registration Authority* (RA). This registration must take place before the CA knows whether or not the user will be issued a certificate. RA verifies the user's identity and issue certificate to the right user. If a user's private key gets compromised (e.g. stolen) the certificate must be revoked from *Certificate Revocation List* (CRL). (Zimmermann 2000: 24.)

3.8. Hybrid Cryptosystem

A hybrid encryption scheme uses public-key encryption to encrypt a random symmetric key, and then proceeds to encrypt the message with that symmetric key. The receiver decrypts the symmetric key using the public-key encryption scheme and then uses the recovered symmetric key to decrypt the message. (Katz 2004.)

3.9. Hash Functions

A hash function H is a transformation that takes a variable-size input *x* and returns a fixed-size string, which is called the hash value h (i.e. h = H(*x*)). The basic requirements for a cryptographic hash function are: the input can be of any length, the output has a fixed length, H(*x*) is relatively easy to compute for any given *x*, H(*x*) is one-way and H(*x*) is collision-free. Main role of a cryptographic hash function is to verify the digital signatures because these functions are faster than DSA.

3.9.1. One-Way Hash Function

A hash function H is said to be *one-way* if it is hard to invert, where "*hard to invert*" means that given a hash value h, it is computationally infeasible to find some input x such that H(*x*) = h. One-way hash functions are also called *message digest algorithms* and it does not require any key. For some purpose they fulfill these conditions:

If it is computationally infeasible to find a message *y* at given *x*, not equal to *x* such that

H(*x*) = H(*y*) then H is *weakly collision-free* hash function or *2^{nd}-preimage resistance.*

If it is computationally infeasible to find any two messages *x* and *y* such that H(*x*) = H(*y*) then H is a *strongly collision-free* hash function or *collision resistance.*

Secure Hash Algorithm SHA-1 (160-bit) for the Internet X.509 PKI, SHA-256 (256-bit) and *Message-Digest* MD2 (128-bit) for certificates, MD4 (128-bit) and MD5 (128-bit) is for other legacy applications are famous examples of keyless hash of function. (Katz 2004.)

3.9.2. Keyed Hash Function

To design the computation of hash function around a secret key is also possible. Keyed hash function has shorter output then keyless hash function; *Message Authentication Codes* (MACs) is an example for this category. There are three different strategies for designing of a message authentication code: either *direct design*, or *use of cipher block* or *keyless hash functions as building blocks*. The HMAC construction is an example of third strategy. If we assume that k is the key and x is our input, then the value for MAC is obtained by double hashing:

$$HMAC\ (x, k)\ =\ h((k \oplus opad)|h\ (k \oplus ipad)|x)) \qquad \textbf{(10)}$$

Where HMAC is keyed hash function, h is hash function, x is variable size input and opad & ipad are just constant values.

The basic use of MAC is to ensure the integrity of a message.

(Katz 2004; Zimmermann 2000: 20-21.)

3.10. Cryptanalysis

Cryptanalysis is the art of deciphering encrypted communications without knowing the proper keys. Attackers can be categorized into Active and Passive categories in the cryptosystem (Forsberg et al. 2010: 19). Active attacker adds, deletes and modifies message, and tries to break other security features along with the confidentiality. While passive attacker only monitors the communication and tries to break confidentiality. Some of the more important ones for a system implementer are described below.

Ciphertext-only attack is when the attacker has no knowledge of contents of the message, and must work from ciphertext only. Modern cryptosystem is not weak against ciphertext-only attacks.

Known-plaintext attack is when the attacker knows or can guess the plaintext for some parts of the ciphertext. The famous modern known-plaintext attack is linear cryptanalysis against block ciphers.

Chosen-plaintext attack is when the attacker is able to know any text he likes encrypted with the unknown key. Differential cryptanalysis against block ciphers or hash functions is a good example of this attack. RSA is also vulnerable to chosen-plaintext attacks.

Man-in-the-middle attack is relevant for cryptographic communication and key exchange protocols, when A and B are exchanging keys for secure communication then an adversary positions himself between A and B on the communication line and intercepts the signals. To prevent this attack we can use digital signature.

Correlation between the secret key and the output of the cryptosystem is the main source of information to the cryptanalyst. In the easiest case, the information about the secret key is directly leaked by the cryptosystem. The correlation idea is essential to cryptography, which provably secures against such attacks.

Attack against or using the underlying hardware is related to hardware implementation of the cryptosystem, attacker tries to obtain the secret key or other kinds information stored on the device.

3.11. Cryptographic Protocols

Cryptographic protocol is a protocol executed on a network where the messages or part of the messages are produced using cryptographic functions. Cryptographic protocols are used to exchange secret information, to achieve a transaction (Electronic Commerce), to vote, to protect copyright on digital content etc. Some famous protocols are mentioned below:

Internet Protocol Security (IPSec): provides a stable and durable base for securing network layer. It supports all of the cryptographic algorithms in use today, and can also accommodate newer, more powerful algorithms as they become available. It has capability to address below mentioned major security issues:

Data origin authentication-verifies that each data was originated by the claimed sender.

Data integrity- verifies that the contents of a data were not modified in transit, either deliberately or due to some errors.

Data confidentiality – keeps secret the content of a message, by using encryption.

Replay protection - ensures that an attacker cannot intercept a data and play it back at some later time.

Automated management of cryptographic keys and security associations - ensures that your VPN policy can be used throughout the extended network with little or no manual configuration. "VPN uses two IPSec protocols to protect data when data passes through this tunnel: *Authentication Header* (AH) and *Encapsulating Security Payload* (ESP). The other part of IPSec is to enable *Internet Key Exchange* (IKE) protocol, or key management. While IPSec encrypts data, IKE supports automated negotiation of *Security Associations* (SAs), and automated generation and refreshing of cryptographic keys" (IBM 2014).

Secure Socket Layer (SSL)/TLS: SSL/TLS works over *Transmission Control Protocol* (TCP) and tunnels other protocols using TCP. SSL protocol, establishes secure connections between clients and server applications by authenticating one or both endpoints of the communication session. It also provides privacy and integrity of the data between client and server applications.

TLS provides the key-hashing for message authentication (HMAC) and enhanced *Pseudo Random Function* (PRF) security improvement. TLSuses *Key-Hashing for Message Authentication Code* (HMAC), which ensures that a record cannot be altered while travelling over an open network. SSL Version 3.0 also provides keyed message authentication, but HMAC is more secure than the MAC function which is used by SSL Version 3.0. And PRF generates key data and is defined by HMAC in TLS. The PRF uses two hash algorithms to assure its security. If either algorithm is exposed, the data will remain secure until second algorithm is not exposed.

(IBM 2014.)

OpenPGP and Secure/Multipurpose Internet Mail Extensions (S/MIME): are standards used public key cryptography to encrypt email. The OpenPGP standard was originally derived from PGP (Pretty Good Privacy), first created by Phil Zimmermann in 1991. Secure/Multipurpose Internet Mail Extensions is a standard for signing of MIME data. It was originally developed by RSA Data Security Inc.

The Secure Shell (SSH): is a protocol for secure network communications, and relatively simple and inexpensive to implement. The initial version, SSH1, focused on providing a secure remote logon facility to replace Telnet and other remote logon schemes that provided no security. SSH also provides a more general client-server capability and can be used to secure network functions such as file transfer and e-mail. SSH2 is a new version and improved version of SSH1.

Kerberos: is for single sign-on and authenticating users against a central authentication and key distribution server. It works by giving authenticated users "tickets", granting them access to various services on the network. When clients then contact servers, the servers can verify the tickets.

Kerberos is a primary method for securing and supporting authentication on a LAN, and for establishing shared secrets (it needs to be used with other algorithms for the actual protection of communication).

(Wheeler 2004.)

4. CELLULAR NETWORK SECURITY

According to Douligeris and Kotzanikolaou (2006), the goal of communication security is protecting information and user during the transmission via communicating medium from unauthorized exposure, modification or interception. In order to achieve the goals of network security in any network, the following steps must be taken into account.

- Scope of the network and assets to be protected, should be defined.
- Possible attacks and threats should be defined.
- Desired security level and security risk should be defined and evaluated.
- Security policies should be defined.
- Security services and mechanisms must be defined and implemented properly.
- Proper placement of security polices, services and mechanism should be assured periodically.

4.1. Global System for Mobile Communications (GSM)

GSM is the most popular mobile phone system in the world and consists of EDGE, 3GSM, and GPSR. EDGE is an upper level component used for downloading audio and video clips, and multimedia messages. GPSR is for web-browsing ("always-on"). 3GSM is the GSM running on third generation standards for multimedia services" (Huynh & Nguyen 2003).

4.1.1. Architecture of GSM

Refer to the **Figure 9**, the entire GSM architecture consists of three basic entities *Mobile Station* (MS)*, Base Station Subsystem* (BSS) and *Network Sub System* (NSS).

The MS consists of *Mobile Equipment* (ME) and *Subscriber Identity Module* (SIM). SIM stores secret information such as *International Mobile Subscriber Identity Module* (IMSI), *Secret Key* (Ki) for authentication, *Personal Identification Number* (PIN) and other subscribers' information. The BSS controls the radio link and provides a radio interface for the rest of the network. The BTS houses the radio transceivers that define a cell and handles the radio-link protocols with the MS. BSC controls several base stations by managing their radio resources, and it is connected to *mobile services switching center* (MSC). NSS is also known as the *Core Network* (CN) and consists of several databases such as VLR, HLR and *Gateway MSC* (GMSC). GMSC is interface between the GSM network and *Public Switched Telephone Network* (PSTN). The MSC provides registration, authentication, location updating, handovers and call routing with the coordination of HLR and VLR. The HLR contains administrative information of registered subscribers in the network with its current location. While the VLR contains only administrative information of subscribers currently located/moved to its area. The *Equipment Identity Register* (EIR) and *Authentication Center* (AuC) contains list of valid *Mobile Equipment* (ME) and subscribers who are authenticated into network. (Elouafiq 2011.)

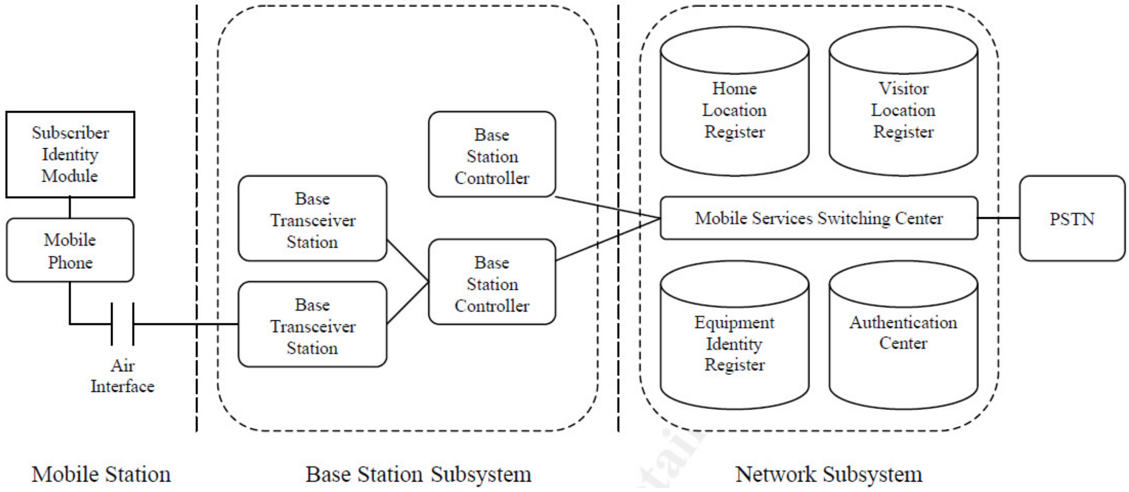


Figure 9. GSM Architecture (InfoSec Reading Room 2001).

4.1.2. Threats to GSM Networks

In general GSM does not meet high security requirements and most attacks are out comes of weak algorithm and architectural flaws. The most important vulnerability of

GSM architecture’s security no needs of network authentication by MS because it was beyond the imagination in 1990s. An attacker would be able to impersonate a network by establishing a faked BTS. GSM cell phone always connects to BTS with the most intense signal. So an attacker is able to connect any GSM device with faked BTS simply by providing the strongest signals, not only able to connect but also able to configure the BTS as an original BTS. That leads a man-in-the-middle attack. The biggest threat is to obtain all data sent by MS in the plaintext. Attacker configures BTS by offering A5/0 (means no encryption). With faked BTS there is possibility of DoS attack as well.

The Smartcard Developer Association and ISAAC security research group discovered a flaw in the COMP 128 algorithm that effectively enabled them to retrieve the secret key Ki from a SIM. The attack was performed on a SIM (physical access) but the same attack is applicable over-the-air. The attack reveals the information about Ki by providing RANDs as a given parameter to algorithm A8. And the SIM was accessed through a smartcard reader connected to a PC.

The anonymity in GSM is provided by using TMSI, which is like a nickname of subscriber locally. An attacker may want some subscriber’s movements and/or follow call samples and so must have the IMSI and the TMSI of the MS. This information may also be used to attack other security assets than anonymity, such as eavesdropping on a specific person. If the attacker can get the IMSI of subscriber or associated current TMSI of a specific person then the anonymity of the user is imperiled. Usually ciphering algorithm A5/1 and A5/2 are rejected; it means there is no encryption at MS.

Over-the-air privacy of GSM telephone conversations is protected by using A5 stream algorithm. This algorithm has two main variants: A5/1 is the “strong” export-limited version used by CEPT-countries, and A5/2 is the “weak” version that has no export limitations. The confidentiality of GSM is protected by the session key Kc with 64-bits length which shows that complexity of brute force attack is 2^{64}. Brute force complexity can be reduced up to 2^{54} by setting last 10 bits to zero.

(Egners et al. 2012: 31-38.)

4.1.3. Security in GSM

To provide an infrastructure with protected access to mobile services and to secure the user’s information are prime objective of GSM security. To achieve authentication, confidentiality, and integrity in GSM network; authentication of subscribers, secure date transfer over the network, protect and secure subscriber’s identity, without SIM a mobile phones can use only emergency service and duplicate SIMS on network are not allowed at all and the keys are securely stored are points to be considered.

In GSM network, security is divided into three different levels. On the very first level, GSM authenticates the subscriber visa SIM and SIM identifies the subscriber. On the second level of security, current location of the subscriber and incoming calling user’s identification is revealed. On the third level encryption of data is done between these two users. Integrity and confidentiality is obtained by establishing secure connection and encrypted the data. (Huynh et al. 2003.)

Encryption Implementation: Now we can take a look at above mentioned three levels:

Authentication at Mobile Station: The GSM network authenticates the identity of the subscriber by utilizing a Challenge/Response mechanism which is described in **Figure 10**. Initially MS receives a 128-bit *Random Number* (RAND). Based upon this challenged RAND along with the *Authentication Algorithm* (A3) and individual subscriber a*uthentication key* (Ki), the MS computes the 32-bit *Signed Response* (SRES). **Figure 11** describes the process of generation of SRES quite clearly. The GSM network repeats the calculation to verify the identity of the subscriber after having the SRES from the subscriber. The individual subscriber authentication key (Ki) is never transmitted over the radio channel. It is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases as previously described. If the received SRES matches with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure indicated to the MS which we can see in **Figure 12**. In the SIM the calculation of the SRES is done and assures enhanced security. The reason is, during the authentication process the confidential subscriber information like the IMSI or the individual subscriber Ki is never released from the SIM. (Margrave)

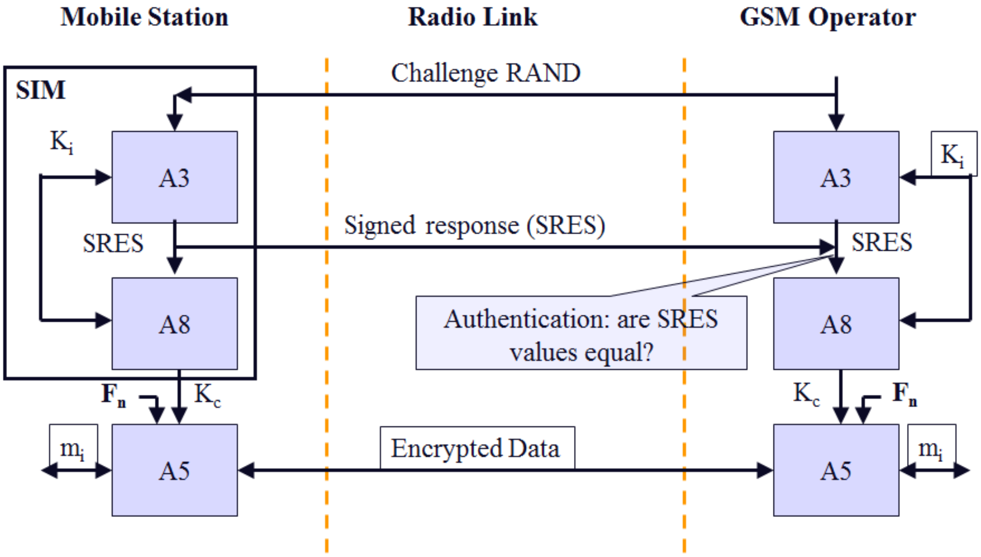


Figure 10. Challenge/Response Mechanism (Stepanov 2003).

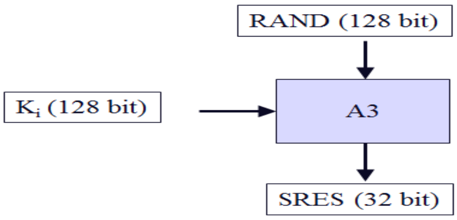


Figure 11. Generation of Signed Response (SRES) (Stepanov 2003).

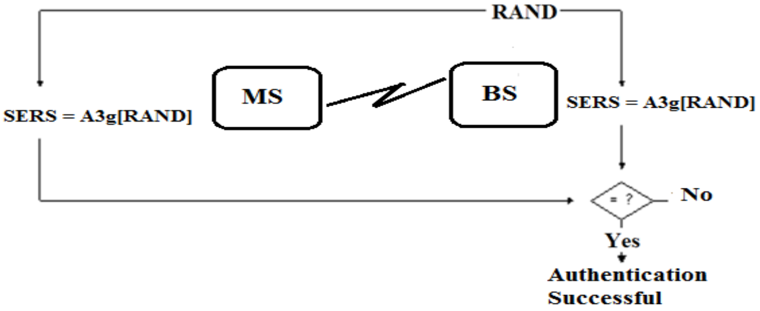


Figure 12. Authentication in the GSM (Margrave).

Signalling and Data Confidentiality: The SIM contains the ciphering key generating algorithm (A8), which is used to produce the 64-bit *Ciphering Key* (Kc). The Kc is computation is shown in **Figure 13**; here RAND is same as in authentication process and Ki is an authentication key of individual subscriber. Later on it will be show that the ciphering key (Kc) is used to encrypt and decrypt the data between the MS and BS. To avoid the eavesdropping and to make the system more resistant, an additional level of security is introduced by changing the ciphering key. The ciphering key may be changed at certain frequency as per requirement of network design and security measurements. By implementing the ciphering algorithm A5, encrypted voice and data communications are accomplished between the MS and the network. Encrypted communication is initiated by a ciphering mode request command from the GSM network. On the base of this command, the mobile station starts encryption and decryption of data using the *ciphering algorithm* (A5) and the *ciphering key* (Kc).

Subscriber Identity Confidentiality: The *Temporary Mobile Subscriber Identity* (TMSI) is key element to ensure the identity confidentiality of subscriber. After the completion of authentication and encryption procedure, the TMSI is sent to the mobile station. The mobile station responds by the acknowledgement of the TMSI. The TMSI is valid in the location area, where it was issued. The *Location Area Identification* (LAI) is required along with the TMSI if need to communicate outside the area. Figure 19 describes TMSI allocation/reallocation process where A5 is ciphering algorithm and Kc is ciphering key.

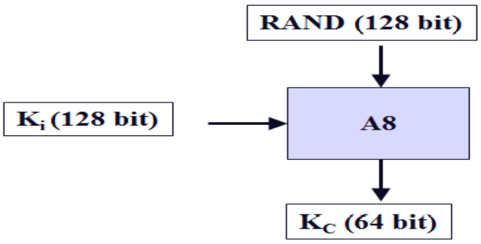


Figure 13. Ciphering Key (Kc) Generation (Margrave).

4.1.4. Cryptographic Algorithm for GSM

A5/1, A5/2 and A5/3 are currently defined encryption algorithms for GSM. European Telecommunications Standards Institute (ETSI) is a custodian of the **A5/4**, **A5/3** encryption algorithms for GSM**.** The A5 algorithms are standardised for mobiles and networks globally interoperability. A5/1 and A5/2 are currently supported by all GSM phones, but most of the networks use A5/1.

Specifications of A5/1 and A5/2 have restricted distribution but the details of the algorithms have been discovered and some cryptanalysis has been published.

COMP128 is hash function which is an implementation of the A3 and A8 algorithms in the GSM standard. This algorithm provides the authentication and security identification of the subscriber on the network.

4.2. General Packet Radio Service (GPRS)

General Packet Radio Service (GPRS) is a data network architecture which is designed to integrate with existing GSM networks and offer mobile subscribers “always on” packet switched data services to corporate networks and the Internet. GPRS has own core network and this core network is attached to the GSM radio network via an open interface. “GSM may utilize the GPRS core network to achieve more efficient performance and the GPRS user may use some of the GSM supplementary services.

However, it is possible to build a GPRS network which is not attached to any GSM network. In that case the GPRS network needs its own radio network" (Huovinen 2007).

4.2.1. Architecture of GPRS

GPRS tries to reuse maximum of the existing GSM network elements, but some new network elements, interfaces, and protocols are required to efficiently build a packet-based mobile cellular network. **Figure 14** summarizes, GPRS requires network elements:

GPRS Mobile Stations: To use GPRS services new Mobile Stations are required because existing GSM phones do not handle the enhanced air interface or packet data.

GPRS Base Station Subsystem: One or more *Packet Control Units* (PCUs) installation and a software upgrade are required by each BSC. Physical and logical data interface to the BSS (for packet data traffic) are provided by PCU. The BTS can also require a software upgrade but not necessarily require hardware enhancements.

GPRS Support Nodes (GSNs): There are two GSNs known as *Gateway GPRS Support Node* (GGSN) and S*erving GPRS Support Node* (SGSN).

Gateway GPRS support node (GGSN): "The GGSN acts as an interface and a router to external networks. The GGSN contains routing information for GPRS mobiles which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic" (Tutorials point 2014).

Serving GPRS support node (SGSN): "The SGSN is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information for charging for the use of the air interface" (Tutorialspoint 2014).

GPRS Backbone: "This is an IP based network used to carry packets between different GSNs. Tunneling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7" (Tutorialspoint 2014).

Routing Area: GPRS introduces the concept of a routing area. This is much the same as a Location Area in GSM, except that it will generally contain fewer cells. Because routing areas are smaller than Location Areas, less radio resources are used when a paging message is broadcast. (Tutorialspoint 2014.)

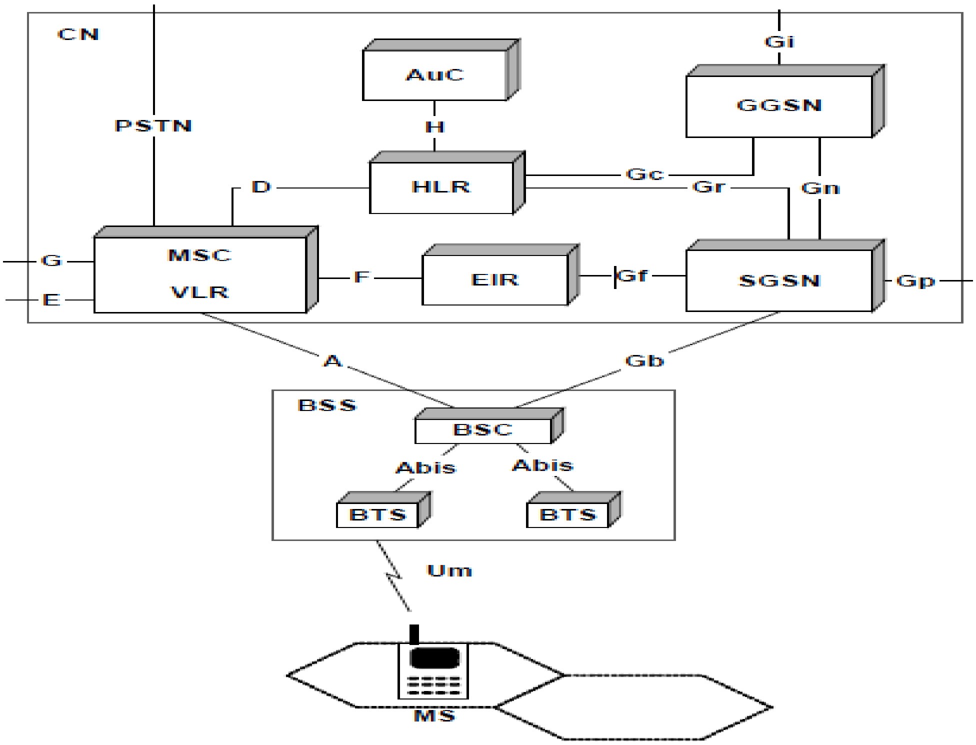


Figure 14. Architecture of GPRS (Merakos & Xenakis 2006).

4.2.2. Threats to GPRS

From **Figure 14**, the Gp interface is a logical connection between PLMNs, used to support mobile roaming data users. The Gi interface is the first interface which sends

MS’s data towards the internet or corporate network, thus it is exposed to public data and corporate customers network. Subscribers are then exposed to all of the harms that we have today on the Internet including viruses, worms, trojan horses, denial of service, attacks, and other malicious network traffic. The basic problem with security threats on the Gp interface is the lack of security inherent in *GPRS tunneling protocol* (GTP). As shown in **Figure 14**, that Gn interface connects an SGSN and the GGSN of the operator and it is exposed to DoS, IP spoofing, privacy and compromise of confidentiality threats. Few possible threats on these interfaces and SS7 are following:

Threats on the Gp Interface: Border Gateway bandwidth saturation, DNS Flood, GTP flood , spoofed GTP, PDP context delete and bad BGP routing information are possible threats against the availability. Spoofed create PDP context request, spoofed Update PDP context request are possible threats against the authentication and authorization. Capturing a subscriber’s data session is possible threat against the integrity and confidentiality.

Threats on the Gi Interface: Gi bandwidth saturation, flooding an MSare possible threats against availability. Data can be seen by third parties if IP Security or application layer security is not being used, so it could be threat against the confidentiality. Data sent over public data networks can potentially be changed by intermediaries and it is considered as integrity’s threats. The source address of network traffic cannot be relied upon for authentication and authorization purposes because the MS or hosts beyond the MS can create packets with any addresses regardless of the IP address assigned to the MS; and it can be a threat against authentication and authorization.

Threats on the Gn Interface: A mobile user (authentic or not) may get access to the GPRS backbone means may perform DoS, IP spoofing, compromise of confidentiality and privacy, etc. User may send massive amounts of data to other users which can be cause of over billing. A malicious may masquerade as a legitimate node (i.e., SGSN, GGSN). Overload a servicing node or change the servicing contexts. A malicious MS in cooperation with a malicious server may perform over billing attacks against an authentic MS. The malicious MS hijacks the IP address of the authentic MS and invokes a download from the malicious server. Then, the malicious MS exits the session and the legitimate MS receive the unwanted traffic.

Threats on SS7: If an attacker gets access to the GPRS backbone s/he may also gain access to the signalling part of the network to listen to critical information and these critical information can be IMSI, TMSI, location information, authentication information, billing data, etc. Perform DoS attacks against the signalling nodes, VLR, HLR, AuC. Retrieve sensitive information that the signalling nodes possess, such as it returns valid authentication triplets.

(NetScreen Technologies Inc. 2002:5-8; Merakos et al. 2006; Perez & Pico 2011: 18-19.)

4.2.3. Security in GPRS

GPRS implements a new set of security mechanisms along with GSM security mechanisms. GSM security mechanisms have been modified to fulfil the requirement of the packet-oriented traffic nature and the GPRS network components. To protect the network against unauthorized access and to protect the privacy of users are primary concerns of GPRS security architecture and it includes following components regarding these concerns.

Subscriber Identity Module – SIM: The mobile subscriber is subscribed with her/his own personalized unique smart card, is known as *subscriber identity module* (SIM). The SIM card authenticates the user by *personal identity number* (PIN). Identification of the user over a network is done by some keys, and the protection of user’s data is done through cryptography. To achieve these functions it contains a set of security objects including: a (4-digit) PIN code, which is used to lock the card preventing misuse; a unique permanent identity of the mobile user, known as IMSI, secret key, Ki, (128 bit) that is used for authentication; and an authentication algorithm (A3) and an algorithm that generates encryption keys (A8). Since the SIM-card of a GSM/GPRS subscriber contains security related sensitive information so it should be manufactured, catered, distributed, and managed in trusted environments.

Subscriber IdentityAuthentication: Authentication for user in GPRS is similar as in GSM. But in GPRS it is executed from the SGSN instead of the MSC as it can be seen from **Figure 14**. Additionally, the authentication procedure performs the selection of the ciphering algorithm and the synchronization for the ciphering. Authentication mechanism uses "authentication triplets" which are received from the HLR/AuC and stored into the SGSN.

Authentication triplets consists of *random numbers* (RAND) between 0 and 2^{128}-1, *signed response* (SRES) which is result of the A3 algorithm used for subscriber authentication, ciphering key (Kc) which is computed using the A8 algorithm and it is used by the *GPRS Encryption Algorithm* (GEA). (Huovinen 2007.)

The first two values from authentication triplets are used as a challenge/response mechanism to authenticate the smart card in the MS as smart card has right key Ki which is related with IMSI. The Kc is used to encrypt all the data between MS and SGSN. Computation of GPRS-Kc and SRES are based on authentication algorithm A3/8 and RAND. For each operator, this authentication algorithm may be individual.

The authentication triplets are sent to the SGSN, which sends RAND to the MS. The MS then use the same authentication algorithm A3/8 to calculate SRES and GPRS-Kc. SERS is sent back to the SGSN, which compares the SRES, returned to it, and the SRES in the authentication triplets. If they are identical, then MS must have the right authentication algorithm A3/8 and Ki. Both the MS and the SGSN also have GPRS-Kc, and both use this key to encrypt the session between MS and SGSN. **Figure 15** clearly describes the authentication and key establishment process. If the MS does not have Ki or authentication algorithm, then it can’t calculate Kc and unable to do encryption. (Brookson 2001.)

Subscriber Identity Confidentiality: It means that a subscriber should have privacy and the identity of user as an IMSI should be confidential when a user is in radio communication. So user’s IMSI needs to replace by a temporary identity which is known as *Temporary Logical Link Identifier* (TLLI). This TLLI is accompanied by a routing area identity (RAI) to avoid the confusions. The relationship between the TLLI and IMSI is saved in database of GPRS.

User and Signalling Data confidentiality: User's data and a 64-bits ciphering key GPRS-Kc is established by A3/8 algorithms as in GSM. Synchronization is performed by a *ciphering key sequence number* (GPRS-CKSN) and synchronization is ensured by ensuring the *GPRS encryption algorithm* (GEA).

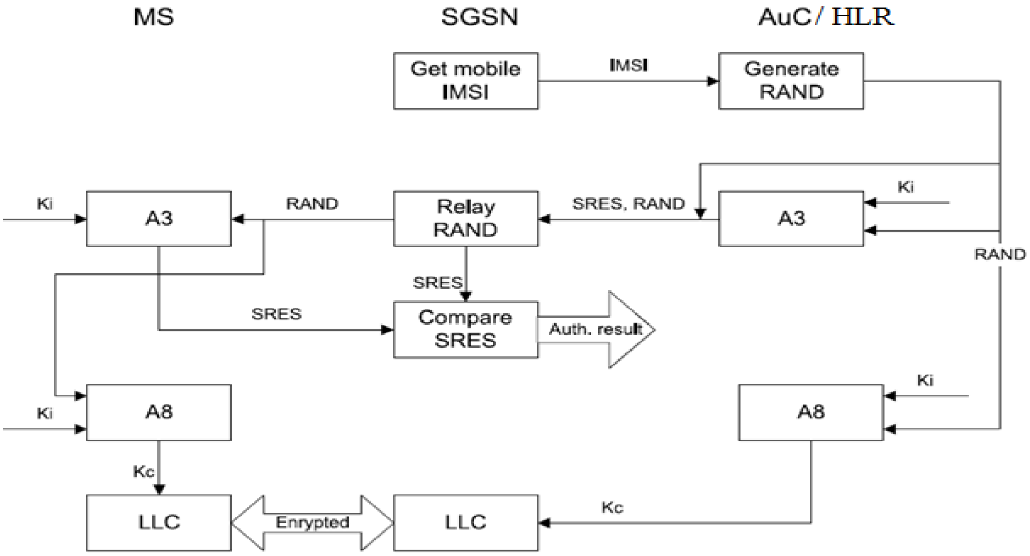


Figure 15. GPRS Authentication and Key Establishment (Brookson 2001).

4.2.4. GPRS Backbone Security

Mobile operators are responsible for backbone inter-network communication security. They deploy private IP addressing and *network address translation* (NAT) to restrict unauthorized access to the GPRS backbone. Unauthorized penetrations for backbone might be protected by applying firewalls at the borders of the GPRS backbone. Firewalls protect the network by enforcing security policies. By using security policies the GPRS operator may be able to restrict traffic in order to protect the MS and the network elements from external attacks and to protect the MS from receiving unrequested traffic.

4.2.5. Cryptographic Algorithm for GPRS

There are seven *GPRS encryption algorithm* (GEA) mentioned in the GPRS specification. Two of them GEA1 and GEA2 have been defined by ETSI’s working group *security algorithms group of experts* (SAGE). (Brookson 2001.)

4.3. Universal Mobile Telecommunications System (UMTS)

The UMTS is evolved version of GSM network through GPRS. The GSM network using *Circuit Switched* (CS) technique for voice communication while GPRS uses *Packet Switched* (PS) technique by having some additional nodes such as SGSN and GGSN. “The UMTS, incorporating GPRS nodes and *UMTS Terrestrial Radio Access Network* (UTRAN), provides both circuit switched and packet switched services with enhanced multimedia applications” (Khan & Ullah 2010).

4.3.1. Architecture of UMTS

A UMTS network comprises of three interacting domains; *user equipment* (UE), *UMTS Terrestrial Radio Access Network* (UTRAN) and *Core Network* (CN) as shown in **Figure 16**. The basic CN architecture for UMTS is based on GSM network with GPRS. All equipment has to be modified for UMTS operation and services. The UTRAN provides the air interface access method for User Equipment. Base Station is referred as Node-B and control equipment for Node-B's is called Radio Network Controller (RNC).

User Equipment (UE) interfaces with the user and consists of *Mobile Equipment* (ME) and *UMTS Subscriber Identity Module* (USIM). ME is the single or multimode terminal used for radio communication and USIM is a smart card that holds the subscriber identity, subscribed services, authentication and encryption keys. UMTS UE can operate in either PS and CS modes or only packet switch mode or only circuit switch mode of operation.

UMTS Terrestrial Radio Access Network (UTRAN) provides the air interface access method for User Equipment and handles all radio related functionality with WCDMA radio interface standard. UTRAN comprises of *Node-B* and *Radio Network Controller* (RNC). Node-B is equivalent to BTS in GSM/GPRS and responsible to for *radio transmission/reception* in one or more cells to/from the UE. It performs and reports radio measurements to the RNC. It also performs the air interface processing such as channel coding, rate adaptation, spreading, synchronization and power control.

Radio Network Controller (RNC) is like a BSC in GSM and responsible for the integrity of the *radio resource* within *Radio Network Subsystem* (RNS) management and control of the Node B's. Radio resource control, admission control, channel allocation, power control settings, handover control, macro diversity, ciphering, segmentation/reassembly, broadcast signalling and open loop power control are functions for RNC.

Core Network (CN) architecture for UMTS is based on GSM network with GPRS. The main function of the core network is to provide switching, routing and transit for user traffic. Core network also contains the databases and network management functions. Following are components of CN:

Home Location Register (HLR) is database located in the user's home system that stores the master copy of the user's service profile and the location of UE on the level of MSC and SGSN.

Mobile Switching Center/Visitor Location Register (3G MSC/VLR) are switch and database that serves the UE in its current location for CS services. The MSC function is used to switch the CS transactions, and VLR function holds a copy of the visiting user's service profile, as well as more precise information on the UE's location within the serving system.

Gateway MSC (3G GMSC) is switch at the point where UMTS is connected to external CS networks. All incoming and outgoing CS connections go through GMSC.

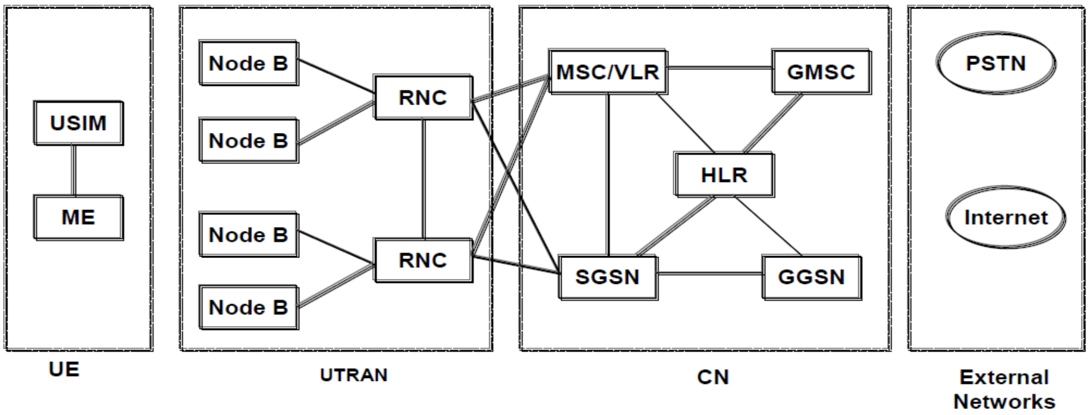


Figure 16. UMTS Architecture (Tipper 2009).

Serving GPRS Support Node (3G SGSN) is similar to that of MSC / VLR but is used for Packet Switched (PS) services. The part of the network that is accessed via the SGSN is often referred to as the PS domain. Upgrade version of serving GPRS support node.

Gateway GPRS Support Node (3G GGSN)is a connection point between a cellular and IP network, which supports 3G networks and other mobile data use by providing access to private and Public Data Networks (PDNs). It is upgraded version of gateway GPRS support Node. (Tipper 2009.)

4.3.2. Threats to UMTS

Threats and attacks against UMTS can be categorized at two levels: one is at UTRAN and another is at core network (CN). In UMTS architecture the radio interfaces between terminal and SN are intending to have threats. The threats related to attacks on radio interface are unauthorized data access, threat against integrity, denial of service and unauthorized service access. Core network traffic between RNCs, MSCs and other networks is not ciphered. MSCs have lawful interception capabilities and access to call data records by design. All switches have to have security measures against unlawful access. Many threats against communication between UMTS network are similar to the threats against on the application layer communication. Threats and attacks against UMTS along with proposed solutions are following:

Denial of service: User de-registration request spoofing, and it can be avoided by implementing integrity protection of critical signalling messages. By doing this, the serving network verifies the de-registration request for integrity and replay. Location update request spoofing can be avoided by protecting location update request against the replay and modification. Camping on a false BS/MS can be avoided by implementing the integrity protection of critical signalling messages. It protects against the denial of service to some degree, as the intruder can't modify signalling messages.

Identity catching: Passive identity catching can be avoided by the using of temporary identities since the impostor has to wait for a new registration or a mismatch in the SN database in order to capture the user's permanent identity in clear text.

Impersonation of the network and thereby eavesdropping:

By suppressing encryption between the target user and the true network: can be avoided by the data authentication and replay protection of a mandatory cipher mode command and it allows the mobile to verify that security has not been suppressed.

By forcing the use of a compromised cipher key: SRNC includes the security capabilities of the MS in a mandatory security mode command. This information lets the MS know that the security capabilities are intact. The MS informs the SN about the unbroken security capabilities in a security mode complete message, leaving the impostor in trouble.

Impersonation of the user:

By the use of a compromised authentication vector & hijacking outgoing calls in networks with encryption disabled: It can be avoided by the presence of a SQN in the challenge helps safeguard against forced re-use of a compromised AV.

Hijacking outgoing calls in networks with encryption enabled: The presence of a SQN in the challenge protects against multiple use of an AV.

Hijacking incoming calls in networks with encryption disabled: The impostor cannot turn off the encryption. Integrity protection of signalling messages at each new RRC connection establishment between MS and VLR/SGSN is mandatory which allows the SN to verify that the request is authentic.

Hijacking incoming calls in networks with encryption enabled: Connections accept message is integrity protected which allows the SN to verify its validity. This means that the impostor cannot accept a connection on behalf of the target user. After the initial connection establishment, periodic integrity protected messages are exchanged during the connection which protects against hijacking of un-ciphered connections.

(Bais, Palensky & Penzhorn 2006.)

4.3.3. Security in UMTS

Infrastructure of security in the UMTS is built on security infrastructure of GSM. “The access security features in UMTS are a superset of those provided in GSM” (Boman, Horn, Howard & Niemi 2002). UMTS authentication objectives are to provide authentication of user to network and vice versa, to establish a cipher and integrity keys, to assure user that these keys were not used before over the network, to take care of intersystem roaming and handover.

According to 3GPP TS 21.133, the security architecture is categorized as:

Network access security: assures confidentiality of user identity (including user and signalling data), integrity protection of critical signalling data, authentication of user and network, and identification of ME.

Network domain security: allows nodes in the operator’s network to securely exchange signalling data, and protects against attacks on the wire line network).

User domain security*:* secures access to mobile stations (by ensuring only authorized access to USIM).

Application domain security: “enables applications in the user and provider domains to securely exchange messages” (Boman et al. 2002).

Visibility and configurability of security*:* "informs the user whether a security feature is in operation and if the use and provision of services should depend on the security feature" (Boman et al. 2002).

4.3.3.1. Security in UTRAN

UMTS has introduced *mutual authentication* between the UMTS subscribers, represented by a smart card application known as the *universal subscriber identity module* (USIM), which extends authentication mechanism of subscriber and network. Mutual authentication is included *Home Environment* (HE) and AuC, *Serving Network* (SN) with VLR and USIM (see **Figure 17)**.

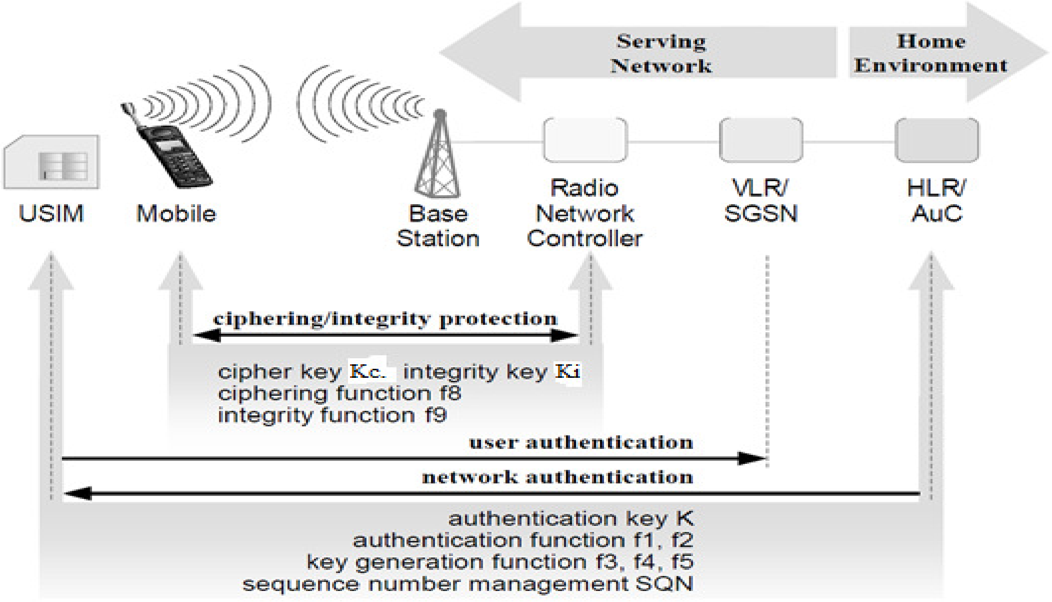


Figure 17. Security Architecture of UMTS (Martin, Pütz & Schmitz 2001).

Mutual Authentication and Key Agreement uses challenge/response mechanism, the SN checks the subscriber's identity (as in GSM) and at the same time the USIM checks that SN has been authorized by the home network. A permanent secret master key K with 128-bits length, shared between the user's USIM and the HE is the significant parameter of the authentication mechanism. The key K is never transmitted over the network and the user has no knowledge of his/her master key. In the mean while temporary keys with 128-bits length for encryption and integrity checking are derived. New keys are derived from the master permanent key K during every authentication process. "It is a basic principle in cryptography to limit the use of a permanent key to a minimum and instead derive temporary keys from it for protection of bulk data" (Abid & Sulistyo 2002).

*Authentication and Key Agreement (*AKA*)* "is based on the assumption that the AuC of the user's home environment and the user's USIM share a user specific secret key K, certain message authentication functions *f1, f2* and certain key generating functions *f3, f4, f5*" (Martin et al. 2001). UMTS AKA is comprised of generation of *Authentication Vectors* (AV) and *AKA mechanism.*

"The key concept in the authentication vector computation is a *one-way function.* Five *f1, f2, f3, f4* and *f5 are* one-way functions used to compute the authentication vector. From *f2* to *f5* take user's permanent secret master key K and an unpredictable challenge random number RAND as input parameters and on other hand *f1* takes four input parameters: K, RAND, sequence number SQN and an administrative *Authentication Management Field (*AMF). The HE/AuC starts with generating a fresh SQN and RAND after receiving an *authentication data request* from SN i.e. SGSN/VLR. And the HE/AuC keeps track of a SQN_{HE} counter for each user. In result, HE/AuC computes the following values (see **Figure 18**):

A message authentication code

$$MAC = f1K(SQN \,||\, RAND \,||\, AMF) \qquad \textbf{(11)}$$

Where f1 is a message authentication function

An expected response

$$XRES = f2K(RAND) \qquad \textbf{(12)}$$

Where *f2* is a (perhaps truncated) message authentication function

A cipher key

$$Kc = f3K(RAND) \qquad \textbf{(13)}$$

Where *f3* is a key generating function

An integrity key

$$Ki = f4K(RAND) \qquad \textbf{(14)}$$

Where *f4* is a key generating function

An anonymity key

$$K_A = f5K(RAND) \qquad \textbf{(15)}$$

Where *f5* is a key generating function

Finally the authentication token is constructed

$$AUTN = SQN \oplus AK \,||\, AMF \,||\, MAC \qquad \textbf{(16)}$$

In equation (**16**) KA is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user" (Martin et al. 2001). The AUTN and RAND are sent to the user by the SN. UMTS authentication vector (RAND, XRES, Kc, Ki, and AUTN) is sent to the SN by the HE.

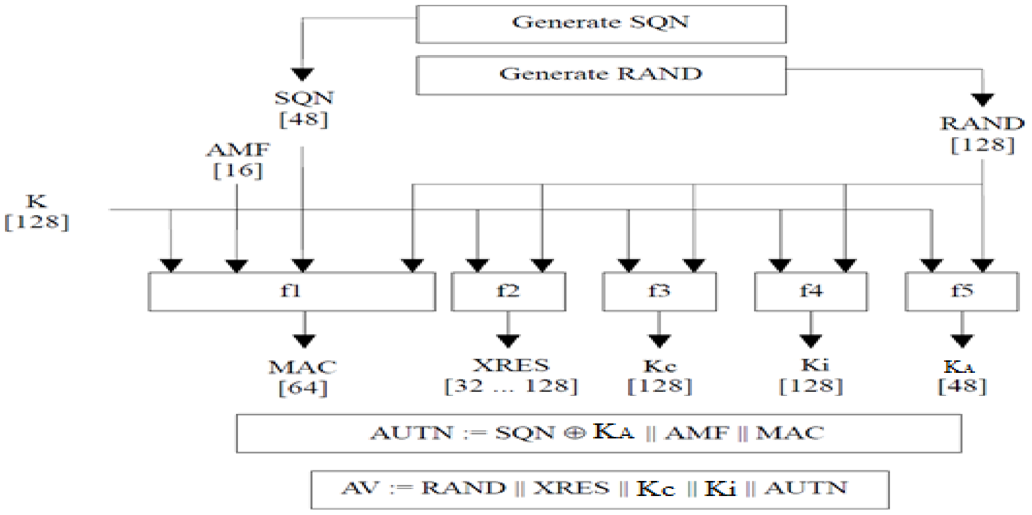


Figure 18. Generation of Authentication Vectors (AV) (3GPP TS 33.102).

The serving network triggers the AKA mechanism by selecting next unused AV from ordered AV array in SN database. This AV node used on *first in first out* (FIFO) order. The SN sends RAND and corresponding AUTN to USIM from the selected AV node. Authentication mechanism is based on identification process by SN. And identification is done by transmitting user's permanent identity (IMSI) or temporary identity (TMSI) to SGSN/VLR. Next to this SGSN/VLR sends an *authentication data request* to the AuC in the HE. AuC can generate the *authentication vectors* (AV) on the behalf of IMSI information and holds master keys of users. These AVs are sent back to SGSN/VLR in the *authentication data response.* This complete process is very well summarized in **Figure 19**.

One AV is needed for each authentication instance in the serving network (SGSN/VLR). The SN sends a *user authentication request* to the terminal, containing parameters RAND and AUTN from the AV. "These parameters are transferred into USIM that exist inside a tamper-resistant environment, i.e. in the UMTS IC Card (UICC)" (Abid, Sulistyo & Najib 2009). The USIM conducts the computation with the stored master key K and RAND and AUTN in the same way of generation of AV in AuC. After computation, USIM verifies whether the parameter AUTN was indeed generated in AuC; if it is a YES case, then computed parameter RES is sent back to SN in the *user authentication response.* And at this stage SN is compares *user response* RES with the *expected response* XRES which is part of the AV. Upon right matching the authentication ends positively.

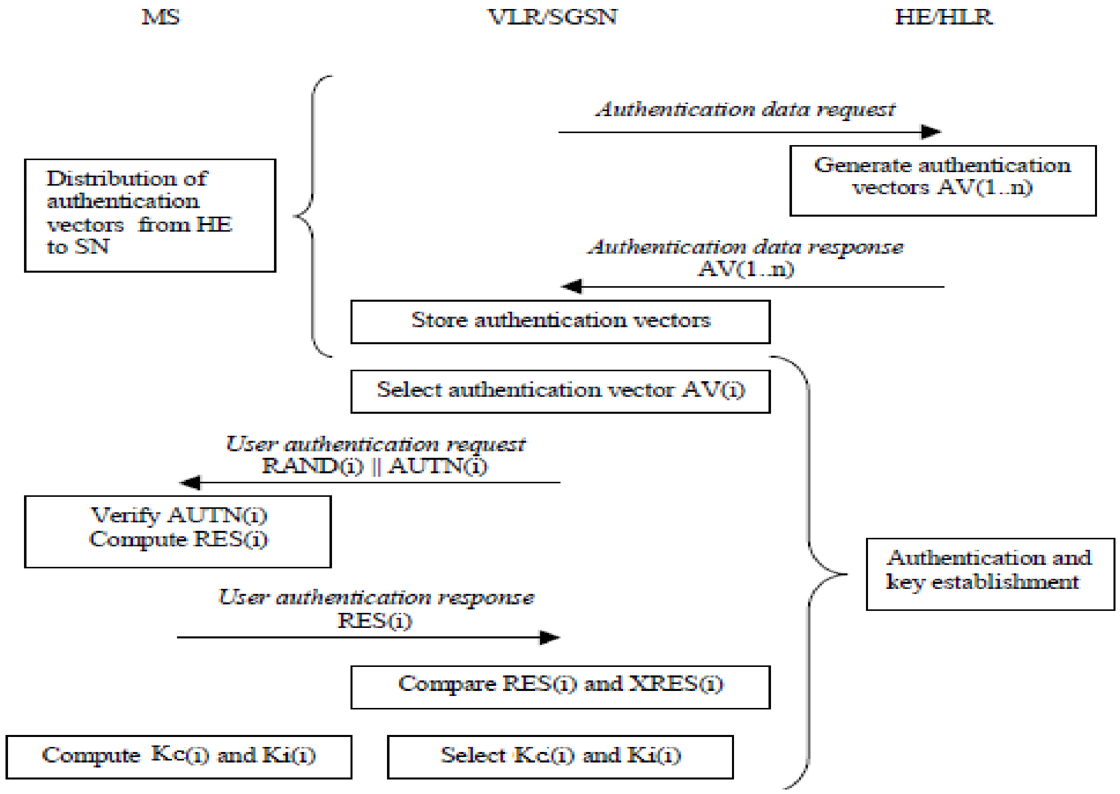

MS
VLR/SGSN
HE/HLR
Authentication data request
Generate authentication vectors AV(1..n)
Distribution of authentication vectors from HE to SN
Authentication data response AV(1..n)
Store authentication vectors
Select authentication vector AV(i)
User authentication request RAND(i) || AUTN(i)
Verify AUTN(i) Compute RES(i)
Authentication and key establishment
User authentication response RES(i)
Compare RES(i) and XRES(i)
Compute Kc(i) and Ki(i)
Select Kc(i) and Ki(i)

Figure 19. Authentication and Key Agreement (AKA) in UMTS (3GPP TS 33.102).

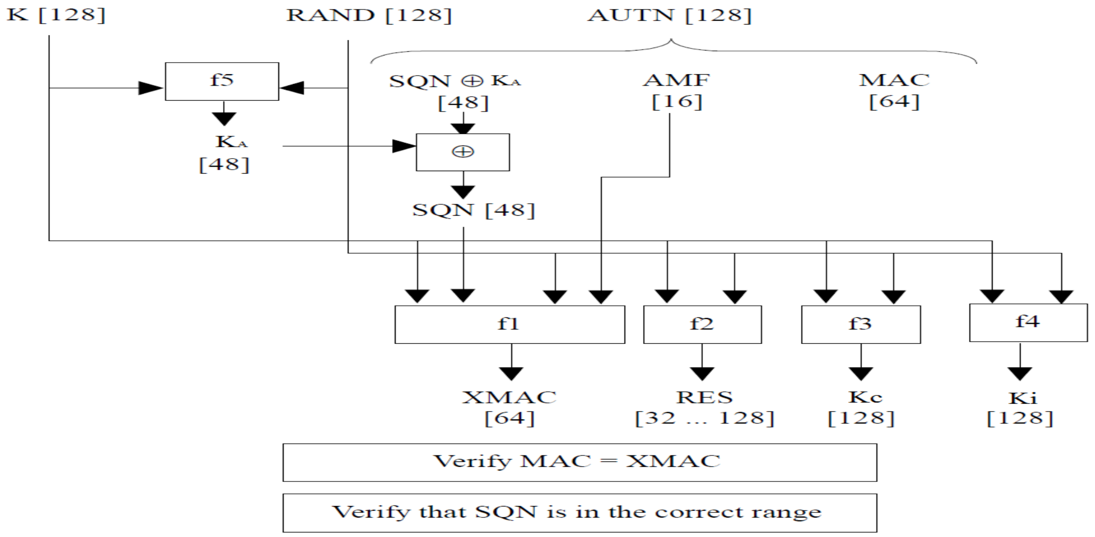


Figure 20. USIM Authentication Function (3GPP TS 33.102).

From **Figure 20**, the USIM computes anonymity key (see equation (**15**)) and retrieves the sequence number.

$$\mathbf{SQN} = (\mathbf{SQN} \oplus \mathbf{K_A}) \oplus \mathbf{K_A} \qquad (\mathbf{16})$$

Where SQN is a sequence number and K_A is same as in equation (**15**).

Then computes expected MAC by computing already defined parameters in above stated equations,

$$\mathrm{XMAC} = f1\mathrm{K}\ (\mathrm{SQN} \parallel \mathrm{RAND} \parallel \mathrm{AMF}) \qquad (\mathbf{17})$$

And later on compares XMAC with MAC. If MAC and XMAC are different, then user sends *user authentication reject* back to the SN to terminate the process. "If the MAC verified successfully, the USIM verifies that the received sequence number SQN is in the correct range" (Martin, Pütz & Schmitz 2001). If the USIM finds SQN is in incorrect range then it sends a s*ynchronizations failure* message back to the SN and USIM terminates the process. "The SN then requests fresh authentication vectors from the HE by transferring the *synchronization failure* message back to the HE. If the SQN is in the correct range then the USIM computes response includes this parameter in a *user authentication response* back to the SN.

$$\mathrm{RES} = f2\mathrm{K}\ (\mathrm{RAND}) \qquad (\mathbf{18})$$

Where RES is response and rest of parameters have been already defined in above stated equations.

Finally the USIM computes the cipher and integrity keys (see equation (**13**) & (**14**)). Upon receipt of the *user authentication response* the SN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The SN also selects the appropriate cipher key Kc and integrity key Ki from the chosen authentication vector" (Martin et al. 2001). And authentication ends positively.

Temporary Identities: With the assumption of being user identified in the serving network by IMSI already. Then the SN allocates a temporary identity (TMSI or P-TMSI) for the association between the permanent identity and the temporary identity. These identities are locally allocated and each SN makes sure to avoid the redundancy of these. User gets this TMSI once the encryption is begun and this used in both uplink and downlink signalling until a new TMSI/P-TMSI is allocated by the network. SN removes old temporary identity after the allocation of new temporary identity. “If allocation acknowledgement is not received by VLR/SGSN it shall keep both the old and new P-/TMSIs and accept either of them in uplink signalling. In downlink signalling, IMSI must be used because the network does not know which temporary identity is currently stored in the terminal. In this case,VLR SGSN tells the terminal to delete any stored TMSI/P-TMSI and a new re-allocation follows” (Abid et al. 2009).

4.3.3.2. Confidentiality (f8)

Ciphering in the access network occurs once user and network are authenticated by each other then there is secure communication. From mutual authentication and AKA section, it is known that there is a shared cipher key Kc between the core network and the terminal after a successfully authenticated. “The ciphering function is performed either in the radio link control (RLC) sub layer (for non-transparent RLC mode) or in the medium access control (MAC) sub layer (for transparent RLC mode)” (Boman et al. 2002). From **Figure 21**, it is clearly seen that ciphering algorithm is f8 to encrypt plaintext. Here plaintext (MAC SDU) is added bit-by-bit to random looking mask data (KEYSTREAM BLOCK), which are generate based on following parameters: the cipher key Kc with 128-bits length, the time-dependent input COUNT-C with 32-bits length, the bearer identity BEARER, the direction of transmission DIRECTION; and the length of the required key stream LENGTH. And final encryption is a very fast bit operation. This type of encryption has advantage that the mask data can be generated even before knowing the actual plaintext. “The decryption on the receiving side is done in exactly the same way since adding ask bits twice has the same result as adding zeroes” (Abid et al. 2009).

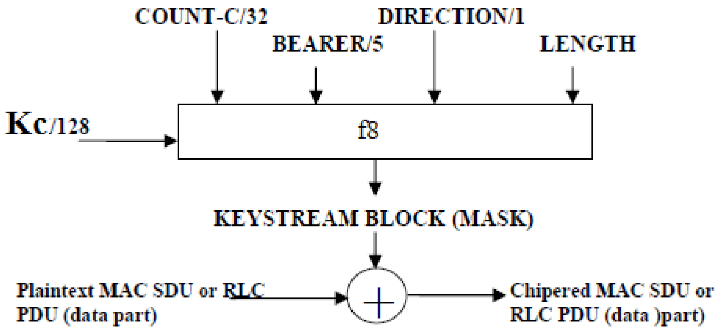

COUNT-C/32
BEARER/5
DIRECTION/1
LENGTH
Kc/128
f8
KEYSTREAM BLOCK (MASK)
Plaintext MAC SDU or RLC PDU (data part)
Chipered MAC SDU or RLC PDU (data)part)

Figure 21. Stream Cipher (Abid et al. 2009).

4.3.3.3. Integrity (f9)

Integrity Protection of Signalling Traffic: Integrity protection is to authenticate individual control messages and is implemented in ME and RNC for user and network respectively. For each individual signalling message, an MAC function is applied to at the RRC layer. Integrity protection is a one-way function controlled by the secret key Ki. The integrity key Ki is generated during the mutual authentication and AKA mechanism and is transferred to the RNC with Kc in security mode command. From **Figure 22**, we can see that integrity algorithm f9 to authenticate the data integrity of an RRC signalling message with output MAC-I. The input parameters to the algorithm are: integrity key Ki with 128-bits length, integrity sequence number (COUNT-I) with 32-bit length and a random value generated by the radio network controller (FRESH) with 32-bit length, both provide replay protection, direction identifier (DIRECTION) to prevent reflection attacks and the RRC signalling message content (MESSAGE). Cipher data MAC-I can be influenced unpredictably if there is any change occurs in the input parameters.

For decryption, the receiver computes an expected MAC-I (XMAC-I) in the same way as the sender computed MAC-I. And verifies the data integrity of the message by comparing XMAC-I to the received MAC-I. This feature also provides the authentication of origin of data.

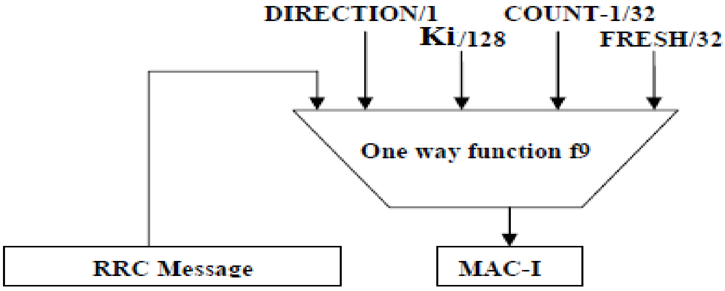


Figure 22. Message Authentication Code (MAC) (Boman et al 2002; Abid et al. 2009).

4.3.4. Security in Core Network (CN)

In CN, the traffic between RNCs and MSCs and other networks is not encrypted and also the earlier used ciphering keys are transmitted between networks. Operators can protect their core network transmission links.

4.3.4.1. Securityin Network Domain (NDS)

“In UMTS Release 99 the core network structure is much like that in GSM and that is why no major enhancement where done in the security of traffic between core networks” (Abid et al. 2009). To address these problems, the CN structure evolves and IP becomes the dominant protocol on the network layer. IPsec protocol provides protection for traffic of network domain by ensuring the confidentiality and integrity of communication in the IP layer. By using IP Sec, interacting parties are able to authenticate each other. But there is still an issue of generating, exchanging and distributing of keys; those are required by confidentiality and integrity algorithms for key management. (Abid et al. 2009.)

4.3.4.2. Securityin Core Network Protocols

GSM uses *mobile application part* (MAP) and the *CAMEL application part* (CAP) for signalling between different network elements. MAP/CAP is running application over the SS7 protocol stack. According to 3GPP’s TS 29.002 specification the UMTS retains evolved GSM core network and its protocols, having consideration that SS7-based transport stack for MAP will be gradually replaced by IP-based transport stack. But there were few difficulties to do so. Therefore to avoid these difficulties it was decided to add a purely IP-based protocols along with MAP and CAP, called *GPRS Tunneling Protocol* (GTP). (Martin et al. 2001.)

4.3.4.3. Security in MAP

MAP secured message is composition of MAP message header, security header and the protected payload. MAP security (MAPsec) provides the confidentiality and integrity of MAP operations in three different modes. Confidentiality and integrity are guaranteed in protection mode 2 of MAPsec, while only integrity is ensured in protection mode 1. And there is no protection at all in protection mode 0. The security header is transmitted in clear-text during all three protection modes. To implement the confidentiality, the payload of original MAP operation is encrypted and s security header is added to show the decryption. To implement the integrity, “a MAC is calculated over the clear-text payload of the original MAP operation and the security header. A time variant parameter is used to protect against replay attacks. The security association for MAPsec are created using IKE protocol. This is done with dedicated key management entities called *Key Administration Center* (KAC), which negotiate key on behalf of all other CN elements in the same network. Integrity of data, authentication of origin of data, protection against replay and confidentiality (optional) are provided by MAPsec. “The following interfaces are defined MAPsec.

Zd-interface: is used to negotiate MAPsec*security associations* (SAs) between PLMNs. The traffic over *Zd* consists only of IKE negotiations. The negotiated MAPsec SAs are valid on a PLMN to PLMN basis.

Ze-interface: is located between MAP-NEs and a KAC from the same PLMN. This interface is used for transport of MAPsec SAs and the relevant security policy information from the KAC to the MAP-NE.

Zf-interface: is located between MAP-NEs. The MAP-NEs may be from the same PLMN or from different P. The MAP-NEs use MAPsec SAs received from a KAC to protect the MAP operations. The MAP operations within the MAP dialogue are protected selectively as specified in the applied MAPsec protection profile. The interface applies to all MAPsec transactions, intra- or inter-PLMN" (Abid et al. 2009).

4.3.4.4. Security in IP-Based Protocol

The UMTS network domain control plane is sectioned into security domains, which typically coincides with the operator borders. *Security gateways* (SEGs) are entities at the borders of the IP security domains used for securing native IP-based protocols are responsible for enforcing the security policy of a security domain towards other SEGs in the destination security domain. In IPsec-based solution, all controlplanes' IP communication towards external networks goes via SEG. 3GPP defines the minimum set of features of IPsec that must be supported for internetworking purposes. These simplifications are: only *Encapsulating Security Payload* (ESP) is used for protection of packets, while AH is not used at all; ESP is always used in tunnel mode; AES is chosen as the encryption algorithm; and IKE is used for key exchange in main mode phase 1 with pre shared secrets.

The NDS/IP specification requires SEGs to implement both versions of the *Internet Key Exchange* (IKE) protocols (IKEv1 & IKEv2), to allow interworking with SEGs and NEs. The specification TS 33.210 describes only the core part that guarantees interoperability between different security domains. (Boman el at. 2002.)

4.3.5. Security in Internetworking between GSM and UMTS

The key element to handle the interoperation between 2G and 3G with securitycontext is different length of keys are being used in these two systems. During 2G authentication 64-bits cipher key Kc is used between SIM or USIM and 2G's SN, while on other hand 3G authentication uses 128-bits cipher Kc and integrity Ki keys between USIM and SN or HE. In order to make it compatible there are specific conversion functions used. Those conversion functions converts or shortens keys length as per requirement. There are basically two scenarios known as *UMTS Subscriber Roaming* (USIM Roaming) and *GSM Subscriber Roaming* (GSIM Roaming). According to 3G2000, TR 31.900 there several subcases under these basic scenarios. “There are five basic entities involved in these scenarios: the security module, the terminal, the radio network, the serving core network and the home network. Each of these entities could be classified into either 2G or 3G” (Forsberg et al. 2010: 51-53).

In **Figure 23**, there are six important cases described. SIM and GSM BSS, SIM application and GSM BSS and SIM and UTRAN B are cases ofGSIM Roaming scenario where a SIM is used as an access module. And *USIM and GSM BSS*, with 2G SN, USIM and GSM BSS, with 3G SN and Pure 3G are cases of USIM Roaming scenario where USIM is used as the security module and in all cases, both the ME and the home network must belong to 3G.

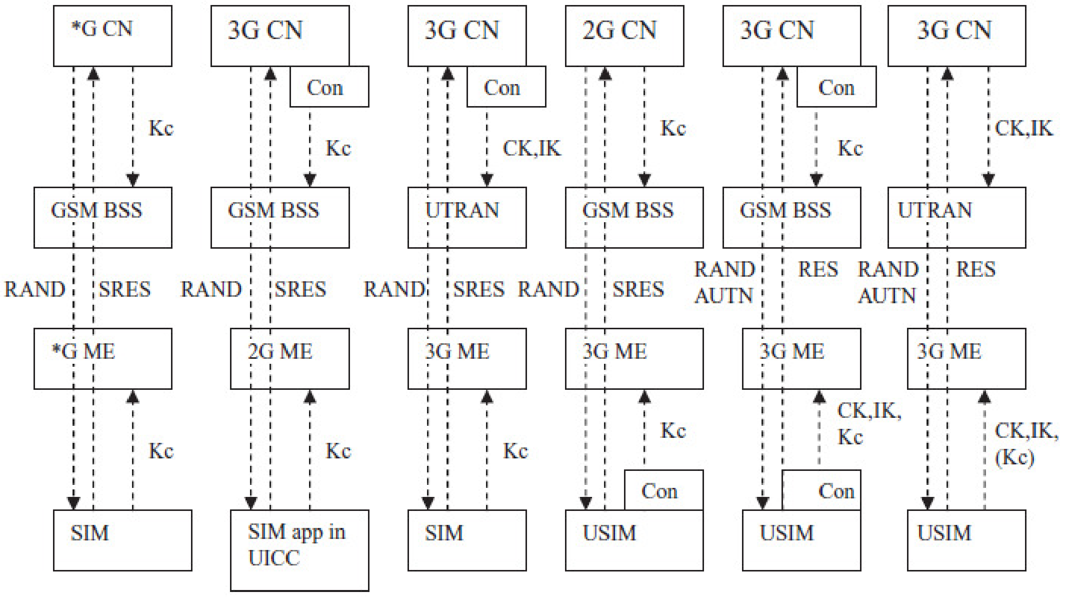


Figure 23. 2G and 3G internetworking Cases (Forsberg et al. 2010: 53)

4.3.6. Cryptographic Algorithm for UMTS

As we have seen already that the security features of UMTS are fulfilled with a set of cryptographic functions and algorithms from *f1* to *f9*. In mutual authentication phase there is no standardized algorithm is required and each operator can choose their own. *MILENAGE* is an example for AKA mechanism (*f1-f5*). A common algorithm called *KASUMI* forms the basis for both the confidentiality algorithm f8 and the integrity algorithm *f9*, which are standardized for use in 3GPP systems. *KASUMI* is a block cipher, which is used in two different operating modes to construct *f8* and *f9*. In traffic and signalling encryption phase there is two *f8* standard algorithms are *UMTS encryption algorithm* UEA1 derived from *KASUMI* and UEA2 derived from *SNOW 3G* available. In message authentication phase there are two standard *f9* algorithms, UEA1 derived from *KASUMI* and UEA2 derived from *SNOW 3G* available. (Gilbert)

4.4. Long Term Evolution/System Architecture Evolution (LTE/SAE)

The term “LTE” comprises the evolution of the UMTS radio access through the *Evolved UTRAN* (E-UTRAN); it is complemented by an evolution of the non-radio aspects under the term “*System Architecture Evolution*” (SAE), which includes the *Evolved Packet Core* (EPC) network. LTE and SAE comprise the *Evolved Packet System* (EPS). EPS uses the concept of EPS carriers to route IP traffic from a gateway in the PDN to the UE. Long Term Evolution (LTE) has been designed to support only packet-switched services. It targets to provide seamless IP connectivity between UE and the *Packet Data Network* (PDN), during the mobility. A carrier is an IP packet flow with an assured Quality of Service (QoS) between the gateway and the UE. The E-UTRAN and EPC set up and release carriers as per an application requirements. (Godin & Palat 2009.)

4.4.1. Architectureof LTE

On broader level the *User Equipment* (UE), *Evolved UMTS Terrestrial Radio Access Network* (E-UTRAN) and *Evolved Packet Core* (EPC) are basic building blocks of LTE network. EPC communicates with PDN in the outside world such as the internet, private corporate networks or the *IP Multimedia Subsystem* (IMS). The interfaces between the different parts of the system are Uu, S1 and SGi as mentioned in **Figure 24**.

User Equipment (UE): The internal architecture of the UE for LTE is identical to UMTS/GSM's ME. The UE comprises *Mobile Termination* (MT), *Terminal Equipment* (TE) and *Universal Integrated Circuit Card* (UICC) modules. Those are responsible of handling all the communication functions, terminating the data streams and running an application known as USIM respectively. A USIM stores user related data such as user's phone number, home network identity and security keys' information; it is quite similar to 3G SIM card.

Evolved UMTS Terrestrial Radio Access Network (E-UTRAN): E-UTRAN is taking care of radio communication between EU and EPC having only *Evolved Base Station* (eNB). In LTE networks mobile communicates with one base station and one cell at a time.

Evolved Base Station (eNodeB/eNB): It sends and receives radio transmissions by using the analogue and digital signal processing functions of the LTE air interface and controls low-level operations by sending signalling messages to its all mobiles. The EPC is connected with eNB via S1 air interface while connected with another eNB via X2 interface. And X2 is useful for signalling and packet forwarding during handover.

The *Evolved Packet Core* (EPC): it comprises of following components:

Home Subscriber Server (HSS): is a central database that contains information about users' SAE subscription data, PDNs to which the user can connect and dynamic information such as the identity of the MME.

Packet Data Network Gateway (P-GW): communicates with the outside world (i.e. PDN) via SGi air interface. Each packet data network is identified by an *Access Point Name* (APN). The P-GW is similar to GPRS's GGSN and UMTS/GSM's SGSN. It is responsible for IP address allocation for the UE, filtering of downlink user IP packets into the different QoS-based bearers and QoS enforcement for guaranteed bit rate bearers.

Serving Gateway (S-GW): serves as a local mobility anchor for the data bearers (when the UE moves between eNBs), serves as a buffer of downlink data (during MME paging) and performs some administrative functions in a visited networks. It also retains the information about the bearers when the UE is in the idle state.

Mobility Management Entity (MME): is the control node that processes the signalling between the UE and CN. It takes care of *Non Access Stratum* (NAS) protocols (running between UE and CN), bearer management and connection management.

Policy Control and Charging Rules Function (PCRF): this component is not mentioned in **Figure 24**, but it is responsible for policy control and decision-making, control of the flow-based charging functionalities, QoS authorization provision.

The interface between the S-GW and P-GW is known as S5/S8. When the two devices are in the same network, there is S5 air interface while they are in different networks then there is S8 air interface.

Non-Access Stratum (NAS): is the functional layer in the UMTS protocol stack between the core network and UE.

Access Stratum (AS): is the functional layer in the UMTS protocol stack between the eNB and the UE.

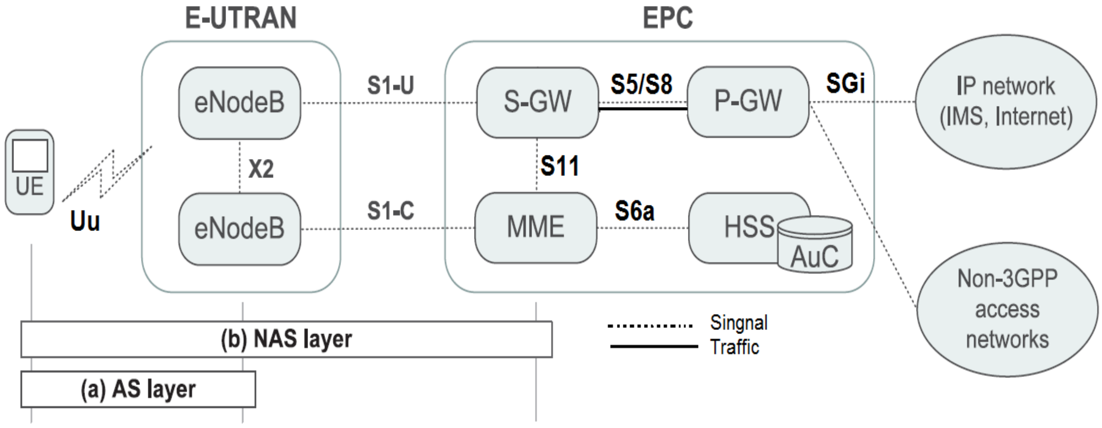


Figure 24. Architecture of LTE (Choi & Han 2014).

4.4.2. Threats to LTE

Open nature of 4G may cause to expose LTE for threats and attacks. A large number of external connectivity points with operators, with third-party applications providers, and with the public Internet; contributes to increase the risk in LTE networks. Also, several heterogeneous technologies accessing the infrastructure, serve as potential security holes in case of lacking of proper implementation of security. In this architecture; multiple service providers share the core network infrastructure, so there is always a chance of compromise of a single provider, which may cause of collapse of the entire network infrastructure. "Service theft and billing fraud can take place if there are third-parties masquerading as legitimate ones. New end-user equipment can also become a source of malicious attacks, viruses, worms, spam mails and calls, and so on. Specially, the *Spam over Internet Telephony* (SPIT), the new spam for VoIP, will become a serious problem just like the e-mail spam today" (Park & Park 2007).

Few more possible VoIP threats are spoofing, data modification, *Session Initiation Protocol* (SIP) registration hijacking, eavesdropping of private conversation (i.e. interception and crypt-analysis of IP packets), and phishing attacks that steal user names, passwords, bank accounts, credit cards, and even social security numbers.

(Park et al. 2007.)

4.4.3. Security Requirements for LTE

UMTS networks are already available with confidentiality of user's ID, authentication and confidentiality of *User Plane* (U-plane) and *Control Plane* (C-Plane) and integrity protection of C-Plane. There are four main requirements for security functions in LTE:

"Provide at least the same level pf security as the 3G network without affecting user convenience. Provide defense against current attacks from the Internet. The security function provided to LTE shall not affect the step-wise transition from 3G to LTE.

Allow continued used of the USIM" (Aono & Zugenmaier 2009).

For last and second last requirements are being satisfied by reusing of 3GPP AKA mechanism and for LTE core network security requirement can be satisfied by applying NDS on IP layer same as 3G. The most important requirement is that LTE must have at least same level of security as UMTS. Following new concepts have been introduced to address the new and modified features of LTE security.

- Hierarchical key setup has been introduced
- Separation between NAS and AS has been introduced
- Concept of forward security has been introduced to limit the threat due to compromised key.
- Additional security functions have been introduced for interconnection between 3G and LTE network.

4.4.4. Hierarchical Key Setup

As it has been mentioned above that, to enhance the security in EPS, a new key hierarchy mechanism is needed. Here is a brief idea of hierarchical key procedure; from **Figure 25** K is master base key for GSM/UMTS/EPS with 128-bits length. CK and IK are cipher and integrity keys derived from master key K with 128-bit length. K_{ASME} is base/intermediated key derived from CK and IK during AKA mechanism with 256-bit length; this is sent as a part of the EPS AVs from HHS including RAND, XRES and AUTN. K_{eNB} is an intermediate key derived from K_{ASME} when UE transits to ECM-CONNECTED states or from K^*_{eNB} during handover with 256-bits length. K^*_{eNB} is derived from K_{eNB} during horizontal handover or from next hop (NH) during vertical handover with 256-bits length. NH is an intermediate key derived K_{eNB} from with 256-bits length to provide forward security. K_{NASint} is an integrity key for NAS signalling derived from K_{ASME} with 256-bits length. K_{NASenc} is a cipher key derived from K_{ASME} with 256-bits length. K_{UPenc} is a cipher key derived from K_{eNB} with 256-bits length, is used for user plane data protection. K_{RRCint} is an integrity key, derived from K_{eNB} with 256-bits length. And K_{RRCenc} is a cipher key also derived from K_{eNB} with 256-bits length. All EPS security keys are 256 bits in length. Only ciphering and integrity keys for AS and NAS algorithms use 128 *least significant bits* (LSB) of the derived keys.

The ciphering and integrity keys are dependent on the algorithms in use. It means, if the security algorithms change for any reason, the associated keys must be re-derived. (Rumney 2013.)

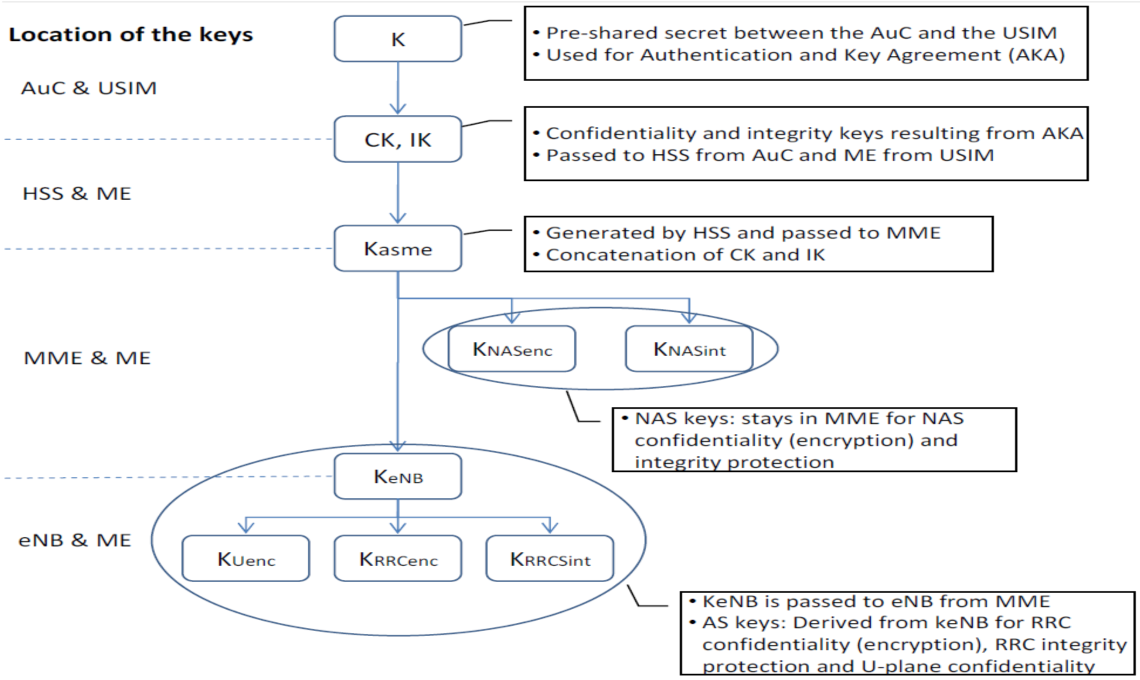

Location of the keys
AuC & USIM
HSS & ME
MME & ME
eNB & ME
K
CK, IK
Kasme
KNASenc
KNASint
KeNB
KUenc
KRRCenc
KRRCSint
• Pre-shared secret between the AuC and the USIM
• Used for Authentication and Key Agreement (AKA)
• Confidentiality and integrity keys resulting from AKA
• Passed to HSS from AuC and ME from USIM
• Generated by HSS and passed to MME
• Concatenation of CK and IK
• NAS keys: stays in MME for NAS confidentiality (encryption) and integrity protection
• KeNB is passed to eNB from MME
• AS keys: Derived from keNB for RRC confidentiality (encryption), RRC integrity protection and U-plane confidentiality

Figure 25. Key Hierarchy (Parsad 2011: 14).

4.4.5. Security in AS and NAS

The AS and the NAS are two levels of security to ensure confidentiality and integrity protection for signalling and user data in the EPS. Signalling and user data confidentiality between the UE and the EPS can be done by ciphering mechanism, while signalling and user data integrity and be done by integrity and replay mechanisms. It is assumed that a large volume of data can be transmitted only when UE is in connected state. NAS security associations are established between UE and EPS in

MME during idle state. AS security associations are established when UE is connected to eNB. We can see in **Table 5** that how AS and NAS security are associated and related with the UE and EPS network elements, specifically the MME and eNB. (Rumney 2013.)

Table 5. AS and NAS Security Association (Rumney 2013).

Security Association	AS	NAS
Termination points	UE and eNB (E-UTRAN)	UE and MME
Ciphering (optional)	RRC signalling (signalling radio bearer) & User plane (data radio bearer)	NAS signalling
Integrity and replay protection (obligatory)	RRC signalling (signalling radio bearer).	NAS signalling
Security protocollayers	PDCP	NAS
Security command procedures	RRC	NAS

Note that there is no requirement for data protection for a user plane tunneled between the eNB and S-GW above network transport layer. NDS can be used for transport layer protection. And integrity and replay protection is not required for user plane transfers between the UE and eNB. (Rumney 2013.)

4.4.6. Security Architecture

After having an idea of LTE's architecture, it came to know that SAE/LTE has flat architecture, ability of interworking with trusted 3GPP and untrusted non 3GPP networks, eNBs are placed in untrusted locations and LTE tries to keep security gaps as local as possible. A system needs extended AKA, more complex key hierarchy, more complex interworking security and extra security for eNB as compared to NB, BTS and RNC in pervious networks.

According to quite many tutorial and white papers, LTE's security can be divided into following five levels (see **Figure 26**):

"Network Access Security (I): The set of security features that provides the UEs with secure access to the EPC and protect against various attacks on the radio link.

Encryption and integrity protection of RRC and NAS signalling, encryption of data radio bearer and mutual authentication between UE and access network are basic radio link security features.

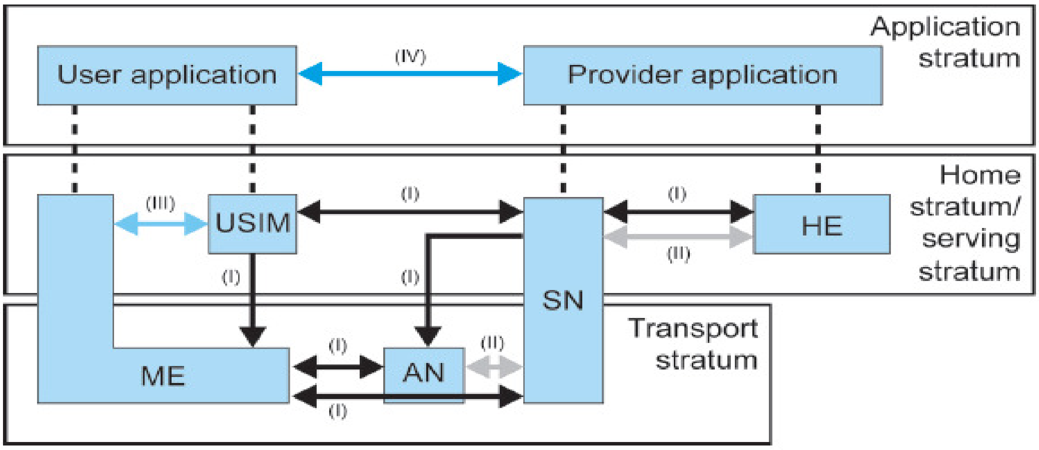


Figure 26. LTE/SAE Security Architecture (3GPP TS 33.401).

Network Domain Security (II): The set of security features that protects against attacks on the wire line network and enable nodes to exchange signalling data and user data in a secure manner. Mainly DNS performs key negotiation by using IKE, security set up the between the SEGs by using Internet Security Association and Key Management Protocol (ISAKMP), encryption, data integrity and authentication by using tunnel mode ESP.

User Domain Security (III): The set of security features that provides a mutual authentication between the USIM and the ME before the USIM access to the ME.

User domain security ensures that ISMI and *International Mobile Equipment Identity* (IMEI) should be confidentially protected; access to the USIM is restricted until the USIM has authenticated by provided PIN and if the inserted USIM has a different IMSI then mobile equipment should go in emergency call mode only.

Application Domain Security (IV): The set of security features that enables applications in the UE and in the provider domain to securely exchange messages.

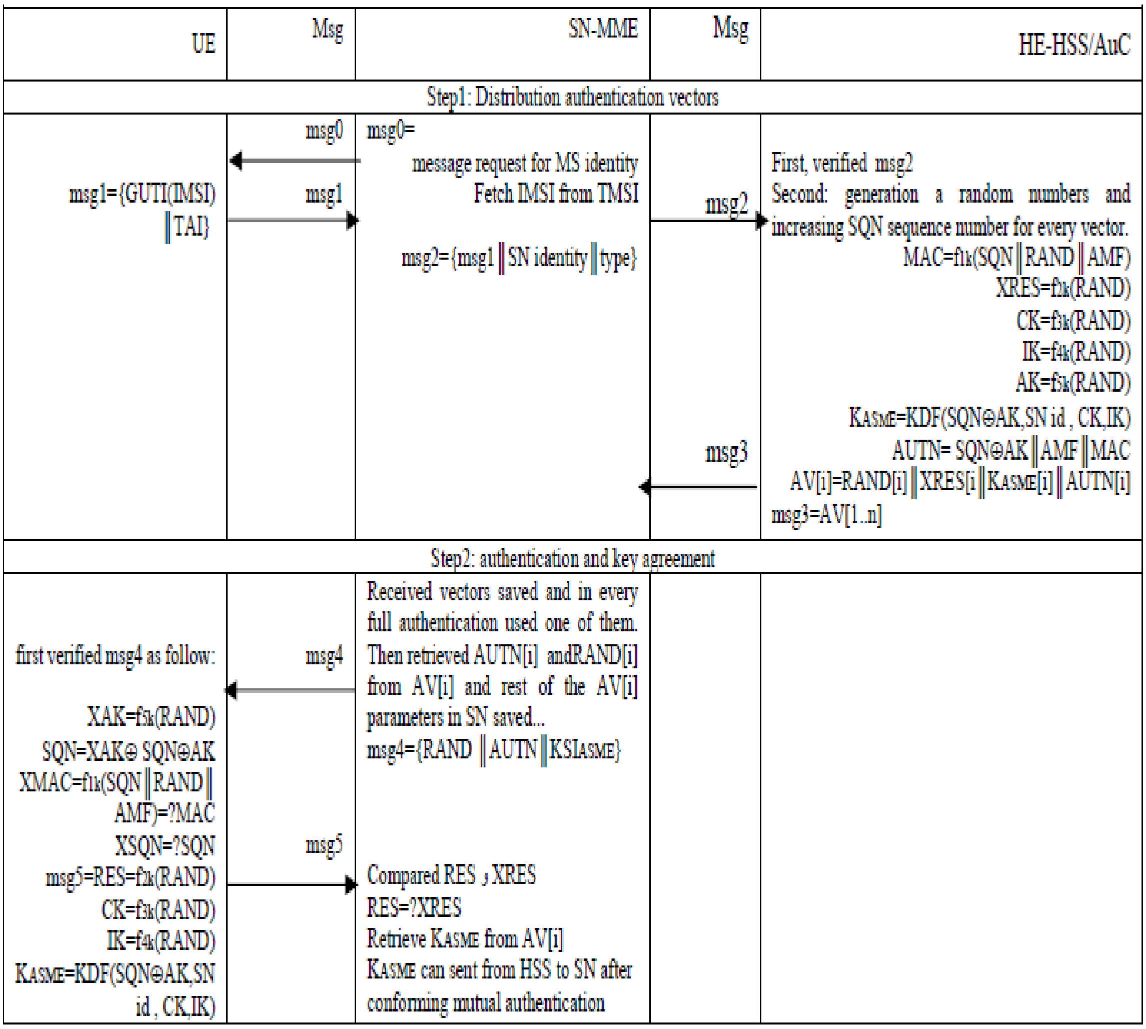
Non 3GPP Domain Security (V): The set of features that enables the UEs to securely access to the EPC via non-3GPP access networks and provides security protection on the radio access link" (Cao, Li, Luo, Ma & Zhang 2013).

4.4.7. Security in LTE Cellular System

As we have seen already in section 4.4.4., that mutual authentication is the most significant security mechanism between the UE and CN. In LTE network it has same significance and it is required between UE and EPC. To achieve this we will use the AKA mechanism with some additional extraordinary features. AKA mechanism generates cipher key (CK) and integrity key (IK) for encryption and integrity protection. Once an UE connects with EPC over the E-UTRAN, the MME represents the EPC to perform a mutual authentication with the UE by the EPS AKA. There several different AKA mechanisms are deployed for non 3GPP access.

From **Figure 27**, we can see that ESP AKA mechanism have several extraordinary features for user access security including *Serving Network Identity* (SN id) has been added to avoid redirection and false base station attacks, at AS level between the UE and eNB and at NAS level between UE and MME there are some new security functions have been introduced, the new root or master key K_{ASME} computed by HHS is introduced which will be delivered to the MME or SN, the *Key Set Identifier* KSI_{ASME} is attached with the user authentication request message transmitted to the UE by the

MME, a new key hierarchy has been introduced to protect the security of the signalling and user data traffic (see **Figure 25**).



UE	Msg	SN-MME	Msg	HE-HSS/AuC
Step1: Distribution authentication vectors				

msg1={GUTI(IMSI)
∥TAI}
	msg0 ←
	msg1 →
		msg0=
		message request for MS identity
		Fetch IMSI from TMSI
		msg2={msg1∥SN identity∥type}
			msg2 →
			msg3 ←
				First, verified msg2
				Second: generation a random numbers and increasing SQN sequence number for every vector.
				MAC=$f1_k$(SQN∥RAND∥AMF)
				XRES=$f2_k$(RAND)
				CK=$f3_k$(RAND)
				IK=$f4_k$(RAND)
				AK=$f5_k$(RAND)
				K_{ASME}=KDF(SQN⊕AK,SN id , CK,IK)
				AUTN= SQN⊕AK∥AMF∥MAC
				AV[i]=RAND[i]∥XRES[i∥K_{ASME}[i]∥AUTN[i]
				msg3=AV[1..n]

Step2: authentication and key agreement				

first verified msg4 as follow:
XAK=$f5_k$(RAND)
SQN=XAK⊕ SQN⊕AK
XMAC=$f1_k$(SQN∥RAND∥
AMF)=?MAC
XSQN=?SQN
msg5=RES=$f2_k$(RAND)
CK=$f3_k$(RAND)
IK=$f4_k$(RAND)
K_{ASME}=KDF(SQN⊕AK,SN
id , CK,IK)
	msg4 ←
	msg5 →
		Received vectors saved and in every full authentication used one of them. Then retrieved AUTN[i] andRAND[i] from AV[i] and rest of the AV[i] parameters in SN saved...
		msg4={RAND ∥AUTN∥KSI_{ASME}}
		Compared RES ,XRES
		RES=?XRES
		Retrieve K_{ASME} from AV[i]
		K_{ASME} can sent from HSS to SN after conforming mutual authentication		

Figure 27. ESP AKA Mechanism (Purkhiabani & Salahi 2012).

For trusted non-3GPP interworking, the UE and the *Authentication, Authorization, and Accounting* (AAA) server implements the *Extensible Authentication Protocol-AKA* (EAP-AKA) or the *improved EAP-AKA* (EAP-AKA') to accomplish the access authentication. EAP-AKA' comprises a new key derivation function that binds the keys derived within the method to the name of the access network, and employs SHA-256 instead of SHA-1. “If an UE connects to the EPC over an untrusted non-3GP access network, the UE and the ePDG needs to perform the IPsec tunnel establishment and further use the Internet Key Exchange Protocol Version 2 (IKEv2) with EAP-AKA or EAP-AKA' to establish the IPSec security associations” (Ma 2010).

4.4.8. Security in Handover Processes

The LTE supports two types of handovers known as intra- and inter-MME handovers. In the intra-MME scenario handover occurs between the source and target NBs managed by same MME via X2 interface (see **Figure 24**), while in the inter-MME scenario handover occurs via the MME without any direct signalling between base stations, here the UE and the MME may decide to run the full EPS-AKA to generate all security contexts from scratch.

Scenario 1: Intra MME Handover

The current eNB and the target eNB are managed by the same MME:

As soon as the UE gets connected state, the eNB switches on the AS security context with AS security mode command and afterwards, AS security is implemented to all communication between the UE and eNB. At this stage MME and UE must generates the $\mathrm{K}_{\mathrm{eNB}}$ and the *next-hop* (NH) parameter respectively. In the initial setup, K_{eNB} is derived directly from master key K_{ASME}, and then gets associated with a virtual NH parameter with a *NH Chaining Counter* (NCC) value to be zero. The UE and the eNB use the K_{eNB} to secure the communication on the air interface. In this case, a new session key K^*_{eNB} is used between the UE and the target eNB which is derived from either the active K_{eNB} or from the NH parameter. We can see in **Figure 28** that a horizontal key derivation is showing generation of K^*_{eNB} from the existing K_{eNB} while a vertical key derivation is showing generation of K^*_{eNB} from the NH. *E-UTRAN’s Absolute Radio Frequency Channel Number-DownLink* (EARFCN-DL) and target *Physical Cell Identity* (PCI) are two additional parameters for K^*_{eNB} generation along with NH.

Scenario 2: Inter-MME Handovers

Mobility between the E-UTRAN and UTRAN/GERAN:

Handover from the E-UTRAN to the UTRAN/GERAN: In this case the UE and the MME first derive a *CK'* and *IK'* from the K_{ASME} and upon receiving *CK'* || *IK'* along with key set identifier *KSI'* from the MME, the target SGSN and the UE shall replace all stored parameters *CK, IK, KSI,* with *CK', IK', KSI'*. UE and the target SGSN use *CK'* and *IK'* to derive the cipher key K_c for GPRS.

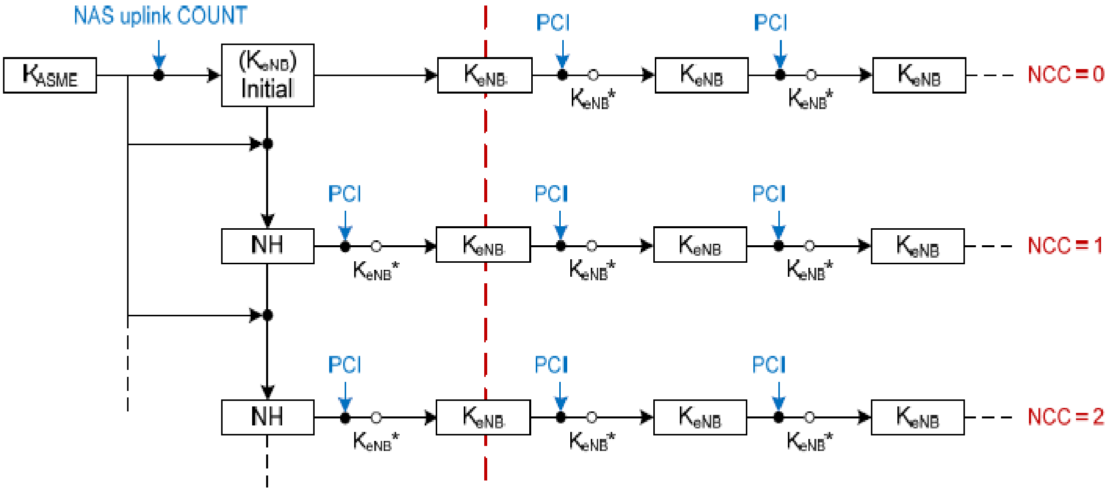


Figure 28. Key Chaining Model for Handover (3GGP TS 33.401).

Handover from the UTRAN/GERAN to the E-UTRAN:

In this case the target MME derives K'_{ASME} from *CK* and *IK* or GPRS K_C received from the SGSN. The UE shall also execute the above same procedure as the MME to derive K'_{ASME}. And the target MME and the UE shall derive K_{eNB} and the corresponding NAS keys according to the key hierarchy of LTE (see **Figure 25**).

Mobility between E-UTRAN and non-3GPP access networks:

There are several different mobility scenarios between heterogeneous access systems in the LTE networks, such ash handovers from trusted or untrusted non-3GPP access networks to the E-UTRAN and handovers from the E-UTRAN to trusted or untrusted non-3GPP access networks. The UE, the target access network and the EPC implement a full access authentication procedure before the UE handovers to the new access network.

(Cao et al. 2013.)

4.4.9. Security in Home NodeB (HeNB)

A HeNB is known as a *Femtocell Access Point* (FAP). It is installed by a subscriber in residence or small office to increase indoor coverage for voice and high speed data service. A HeNBs incorporate the capabilities of a standard eNB. There are closed access, hybrid access and open access available for HeNB. A HeNB gets connected to the EPC over the Internet via the broad band backhaul. Security features of the HeNB are categorized as: HeNB access security, Network domain security, HeNB service domain security, UE access control domain security and UE access security domain. (Cao et al. 2013.)

4.4.10. Security in Machine Type Communication (MTC)

MTC is the Machine to Machine (M2M) data communication without human interaction. The MTC devices can communicate with one/more MTC servers over the LTE networks. And can also communicate directly with each other without contacting any MTC servers. MME used EPS AKA mutual authentication mechanism to enable the secure communication between the MTC device and network. MTC security architecture is divided into following areas.

Security for the MTC between the MTC device and 3GPP network: such as security measurements between the MTC device and RAN, E-UTRAN/UTRAN /GREAM; between MTC devices and MME; and between MTC devices and MTC-IWF for 3GPP access while ePDG for non 3GPP access. (Cao et al. 2013.)

4.4.11. Security in IMS

The IMS is expected to be a key component of the LTE/SAE architecture. IMS is actually overlay architecture to provide the LTE networks with multimedia services. An UE needs a new *IMS Subscriber Identity Module* (ISIM) located within the UICC for multimedia services. The IMS authentication keys and functions at the user side are stored at the ISIM. Experimental work of this thesis is related to security measurement during SRVCC, so background information of IMS and SRVCC are given below. From **Figure 29**: the key elements in the IMS are the SIP proxies, *Call Service Control Functions* (CSCF), which consists of *Proxies-CSCF* (P-CSCF), *Interrogating-CSCF* (I-CSCF) and *Serving-CSCF* (S-CSCF).

(Cao et al. 2013.)

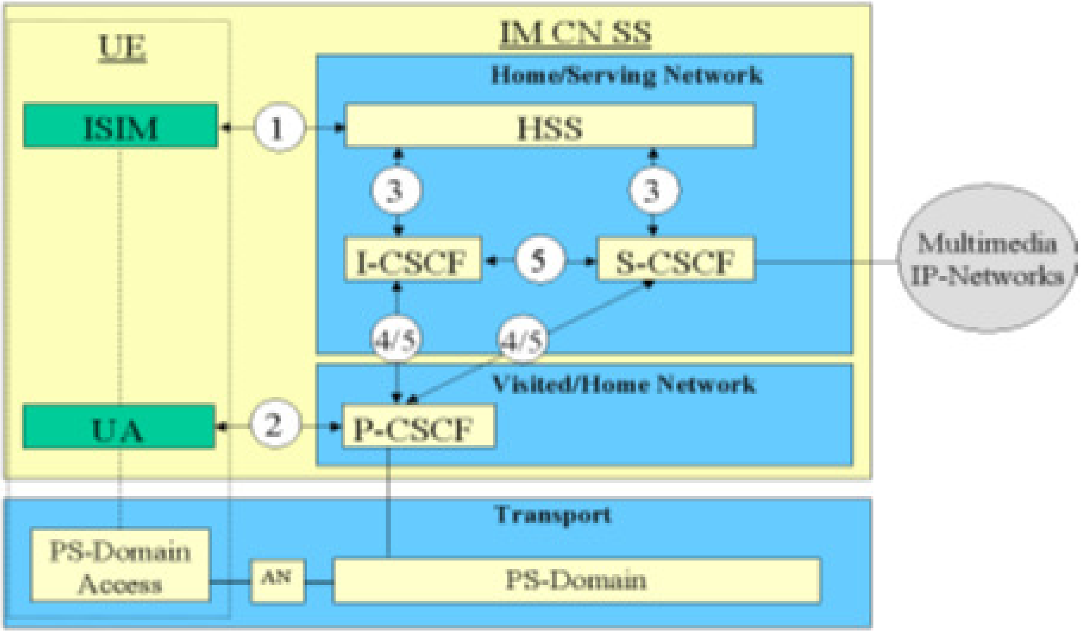


Figure 29. IMS Security Architecture (3GPP TS 33.203).

4.4.12. Cryptographic Algorithms for LTE

The 128-EEA1 and 128-EIA confidentiality and integrity algorithms for LTE are identical to the 3GPP confidentiality and integrity algorithms UEA2 and UIA2. The confidentiality algorithm 128-EEA3 is a stream cipher that is used to encrypt/decrypt blocks of data under a confidentiality key. The block of data can be between 1 and 2^{32}-bits. The integrity algorithm 128-EIA3 is a MAC function that is used to compute the MAC of an input message using an integrity key IK. The message can be between 1 and 65504-bits.

The EPS Encryption Algorithms (EEA) are specified in 3GPP TS 33.401 as:.

"00002" 128-EEA0 Null ciphering algorithm

"00012" 128-EEA1 SNOW 3G

"00102" 128-EEA2 AES

The EPS Integrity Algorithms (EIA) are also specified in 3GPP TS 33.401.

"00012" 128-EIA1 SNOW 3G

"00102" 128-EIA2 AES

EEA0 specifies the null ciphering algorithm, which means that ciphering is not activated, hence no confidentiality protection is offered.

EEA2/EIA2 is based on the AES. The selection of EEA/EIA by AS and NAS may not be the same, hence selections are independent. RRC and U-Plane in AS uses the same selected EEA for Ciphering.

(3GPP TS 33.401; ETSI/SAGE V1.7 2011; ETSI/SAGE V1.1 2011 & ETSI/SAGE V2.0 2011.)

5. SECURITY MEASUREMENTS FOR SRVCC

LTE networks are being deployed alongside legacy networks (GERAN/ UTRAN/ 1xRTT), the ability for multimode mobile devices to connect to different network technologies is an important part of providing the best possible mobile voice and data experience to customers. However, adoption of LTE and its all-IP Radio Access Network (RAN) has introduce one of the key challenges of LTE deployment that is "delivery of voice services in an all-IP network". To overcome these challenge, several approaches were investigated by the wireless industry including: *Voice Over LTE* (VoLTE), Circuit Switched Fallback (CSFB), *Simultaneous Voice and LTE* (SVLTE) and *Voice over LTE via GAN* (VoLGA).

VoLTE was developed by collaboration between over forty operators such as AT & T, Verizon Wireless, Nokia and Alcatel-Lucent etc. In 2010, GSMA announced to support VoLTE. It allows call continuity with cost, size, and battery efficiency advantages over dual radio solutions such as SVLTE. It is based on the IMS network, with voice services being delivered as data flows within the LTE data bearer. As a result, SRVCC is required in order to execute a seamless handover of a voice call from an LTE network to a 3G network and provide continuity for traditional circuit-switched networks.

According to 3GPP TS 23.216 V8.8.0 specification, "*Single Radio Voice Call Continuity* (SRVCC) refers to the voice call continuity between IMS over PS access and CS access for calls that are anchored in IMS when the UE is capable of transmitting/receiving on only one of those access networks at a given time". In simple words, it is for handover between a packet call in LTE and a circuit call in a legacy system.

5.1. Architecture of SRVCC

The simplest architecture of SRVCC is shown in **Figure 30**. In this figure, "E-UTRAN makes the handover decision based on the measurement report from UE and selects the target cell. MME for the LTE access-network receives the handover request from E-

UTRAN with the indication that this is for SRVCC handling, and then triggers the SRVCC procedure" (LinYing & WenYuan 2012). The UE indicates its SRVCC capability to the MME during the mobility management procedures which in turn provides a 'SRVCC operation possible' indication to the eNodeB. Whenever an SRVCC capable UE is losing LTE coverage, the eNodeB detects it and triggers handover procedure towards the MME. MME supports a new Sv interface towards the MSC server enhanced for SRVCC, and forwards the SRVCC handover request towards the target UMTS/GERAN via the MSC server. The MSC server acts as an *Inter Working Function* (IWF) and prepares the target side for handover. In parallel to the target preparation it also triggers session transfer procedure at the *Services Centralization and Continuity Application Server* (SCC AS). The target UMTS/ GERAN preparation is completed and the core network performs a handover of the UE to the target side by sending a handover command, also the IMS session transfer is completed in parallel. The eNodeB needs enhancement in order to prepare appropriate information for the target RAN and trigger SRVCC handover. The MME separates the bearer carrying voice from other bearers and also signals MSC server about the SRVCC handover. The MSC server acts like an IWF and legacy MSCs needs enhancement or a new MSC server itself can be deployed. (Paisal 2010.)

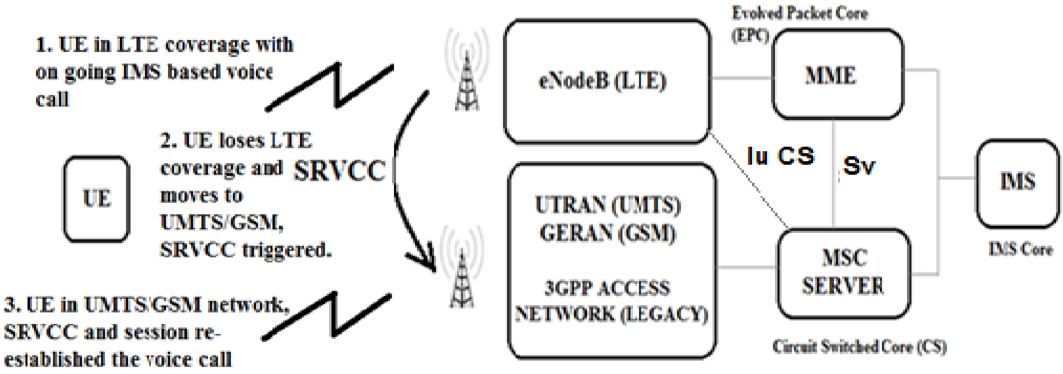

1. UE in LTE coverage with on going IMS based voice call
2. UE loses LTE coverage and moves to UMTS/GSM, SRVCC triggered.
SRVCC
3. UE in UMTS/GSM network, SRVCC and session re-established the voice call
UE
eNodeB (LTE)
UTRAN (UMTS)
GERAN (GSM)
3GPP ACCESS NETWORK (LEGACY)
Evolved Packet Core (EPC)
MME
Iu CS
Sv
MSC SERVER
Circuit Switched Core (CS)
IMS
IMS Core

Figure 30. SRVCC Architecture (Qualcomm 2012).

5.2. Security in SRVCC

5.2.1. Security Keys Derivation during SRVCC Procedure

After reviewing SRVCC's architecture (see section 5.1) and security in handover processes (see section 4.4.8.), now in this section we will see that how security keys are being derived and used during handover between E-TRAN and UTRAN-(CS)/GREAN with SRVCC approach.

According to 3GPP TS 33.401 V9.4.0 Release 9: In this procedure, the MME selects the current NAS downlink COUNT value for the handover and then increase this stored value by 1. The MME and the UE derive a confidentiality key CK_{SRVCC}, and an integrity key IK_{SRVCC} from K_{ASME} of the current EPS security context and the selected NAS downlink COUNT with the help of a one-way key derivation function KDF. The KDF returns a 256-bit output, comprising of the 128 MSBs (identified with $CK_{SRVCC)}$ and the 128 LSBs (identified with $IK_{SRVCC)}$. The MME also provides the 4 LSB of the selected NAS downlink COUNT value to the source eNodeB, which then includes the bits to the HO Command to the UE. The UE uses the received 4 LSB and its stored NAS downlink COUNT to estimate the NAS downlink COUNT selected by the MME. The UE ensures that the estimated NAS downlink COUNT has not been used to calculate a CK' and IK' in a previous successful or unsuccessful PS or CS (SRVCC) handover. If the estimated NAS downlink COUNT is greater than all the estimated NAS downlink COUNTs either used by the UE for key derivation in a handover or received in a NAS message that passed its integrity check, the UE updates its stored NAS downlink COUNT as though it has successfully integrity checked a NAS message with that estimated NAS downlink COUNT. And the stored NAS downlink COUNT is never be decreased. UE and MME assign the value of eKSI to KSI. MME transfers CK_{SRVCC}, IK_{SRVCC} with KSI and the UE security capability to the MSC server enhanced for SRVCC. The MSC server enhanced for SRVCC replaces all the stored UTRAN CS key parameters CK, IK, KSI, if any, with CK_{SRVCC}, IK_{SRVCC}, KSI received from the MME when the SRVCC handover is successful. The UE replaces all the stored UTRAN CS key parameters CK, IK, KSI, if any, with CK_{SRVCC}, IK_{SRVCC}, KSI in both ME and USIM. $START_{CS}$ complies with the rules in 3GPP TS 25.331.

5.3. Case Study & Verification of Test Data Sets

After having the concept of key derivation during SRVCC handover. Here are few scenarios, where voice call is being anchored in IMS and mobility is being occurred from E-UTRAN to UTRAN(CS)/GERAN, triggered SRVCC.

5.3.1. Case Study

Scenario 1: SRVCC handover (also known as inter-RAT) from E-UTRAN to GERAN with non lu mode and without *Data Transfer Mode/Packet Switched Handover* (DTM/PSHO) support.

From **Figure 31**, the source MME is a core node of the LTE network, and a target MSC and a target SGSN are core nodes of the GSM network. A *MSC* server/media gateway (MGW) is an interfacing core node between the LTE and GSM networks. The SRVCC handover without DTM/PSHO support follows mentioned below steps:

1: E-UTRAN takes decision to trigger the SRVCC handover to the GERAN based upon UE measurement reports.
2: E-UTRAN sends a *Handover Required* message along with a *SRVCC handover indication* to the MME.
3: Based upon *Quality of Service Class Indicator* (QCI) (which is associated with a voice bearer) and the *SRVCC handover indication*, the MME separates the voice bearer from non-voice bearers and starts a PS-CS handover procedure for the voice bearer only towards MSC Server.

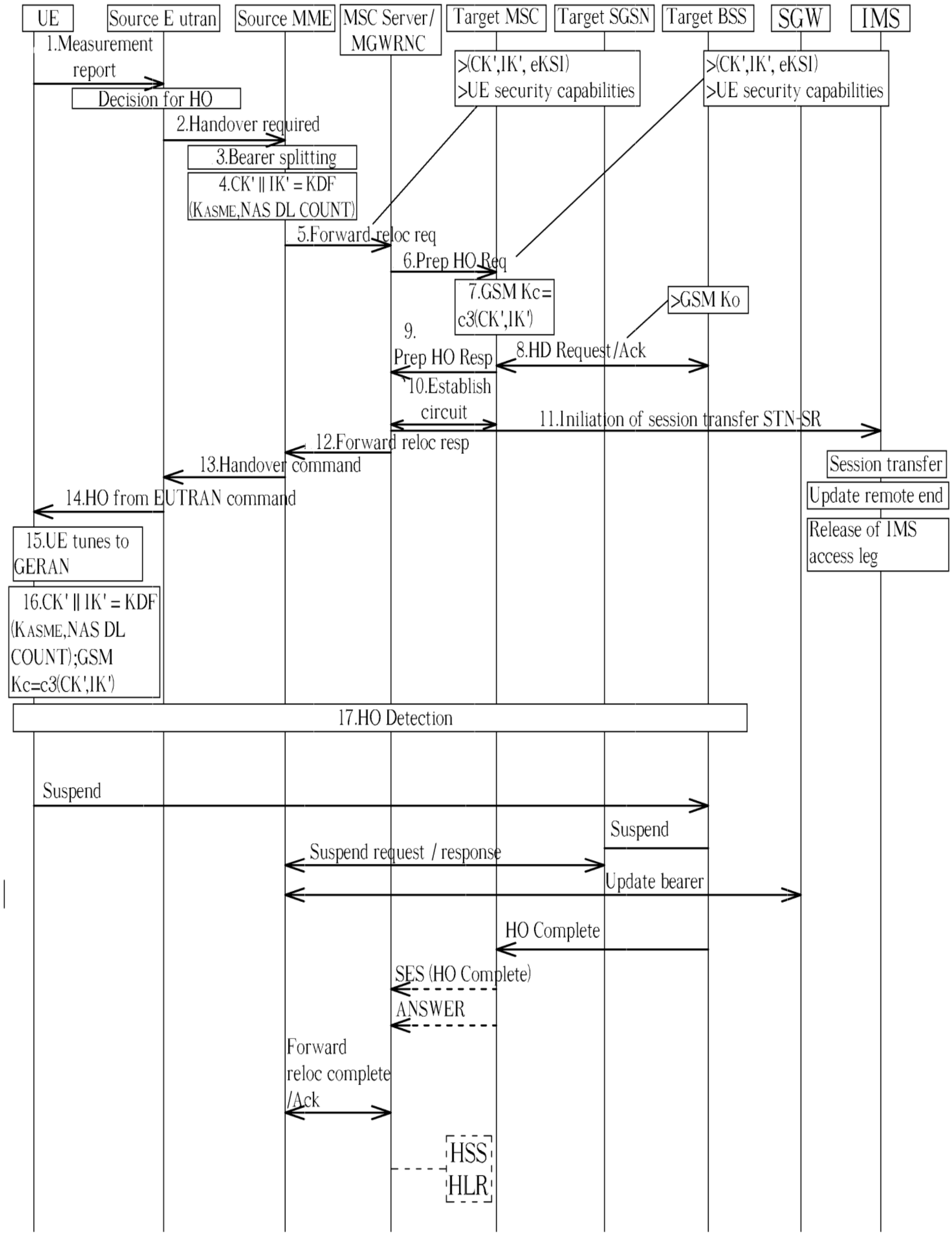


Figure 31. SRVCC Handover from E-UTRAN to GERAN (with non-lu mode and without DTM/PSHO support) (Wu 2010).

4: At this stage the MME derives a CK' and an IK' from a K_{ASME} stored in the MME and a NAS DL COUNT with the KDF (see section 5.2.1) .

5: Now MME sends a *Forward Relocation Request* message along with MM context to the MSC Server. The MM Context contains the CK', the IK', an eKSI, and UE security capabilities.

6: The MSC Server inter-works the PS-CS handover request with a CS inter-MSC handover request by sending a *Prepare Handover Request* message to the MSC. Here the *Prepare Handover Request* message transfers the security information of the MM Context.

7: MSC derives a GSM ciphering key Kc from the (CK', IK') by applying a conversion function *c3*.

8: MSC performs resource allocation by exchanging *Handover Request/Acknowledge* messages with the target BSS. And BSS gets the Kc from the *Handover Request* message.

9: MSC sends a *Prepare Handover Response* message to the MSC Server in response to the *Prepare Handover Request* message received in 6.

10: A circuit connection is established between the target MSC and the MGW (associated with the MSC Server).

11: The MSC Server starts a Session Transfer by sending an *Session Transfer Number for SRVCC* (STN-SR) message towards an IMS. The downlink flow of Voice packets is switched towards a CS access leg.

12: The MSC Server sends a *Forward Relocation Response* message to the MME.

13: The source MME sends a *Handover Command* message to the source E-UTRAN. This message includes information about the voice component.

14: E-UTRAN sends a *Handover from E-UTRAN Command* message along with CS connection configuration.

15: The UE adjusts with a frequency spectrum of the GERAN system.

16: According to the CS connection configuration, the UE derives (CK_{CS}, IK_{CS}) from the K_{ASME} and the NAS DL COUNT with a KDF, and then derives a GSM ciphering key Kc from the derived (CK_{CS}, IK_{CS}) key sets by applying the conversion function *c3* (

same as in step 7).

17: And finally the UE performs handover detection at the target BSS.

(Wu 2010.)

Scenario 2: SRVCC handover from E-UTRAN to UTRAN with PSHO support.

Refering **Figure 32**, in this scenario the source MME is a core node of the LTE network as like before, and a target RNS and a target SGSN are core nodes of the UMTS network. A MSC server/MGW is an interfacing node between the LTE and UMTS systems. The SRVCC handover is having the following steps:

1: E-UTRAN takes decision to trigger the SRVCC handover to the GERAN based upon UE measurement reports.

2: E-UTRAN sends a *Handover Required* message along with a *SRVCC handover indication* to the MME.

3: Based upon the *QCI* (associated with a voice bearer) and the *SRVCC handover indication*, the MME starts a PS-CS handover procedure for the voice bearer only towards the MSC Server after spliting the voice bearer from non-voice bearers.

4: MME derives a CK' and an IK' from a K_{ASME} stored in the MME and its NAS DL COUNT with the KDF (see section 5.2.1)

5: The MME sends a *Forward Relocation Request* message along with MM context to the MSC Server. The MM Context comprises of the CK', the IK', an eKSI of the MME, and UE security capabilities.

6: The MSC Server inter-works the PS-CS handover request with a CS inter-MSC handover request by sending a *Prepare Handover Request* message towards the target MSC. The *Prepare Handover Request* message transfers the security information

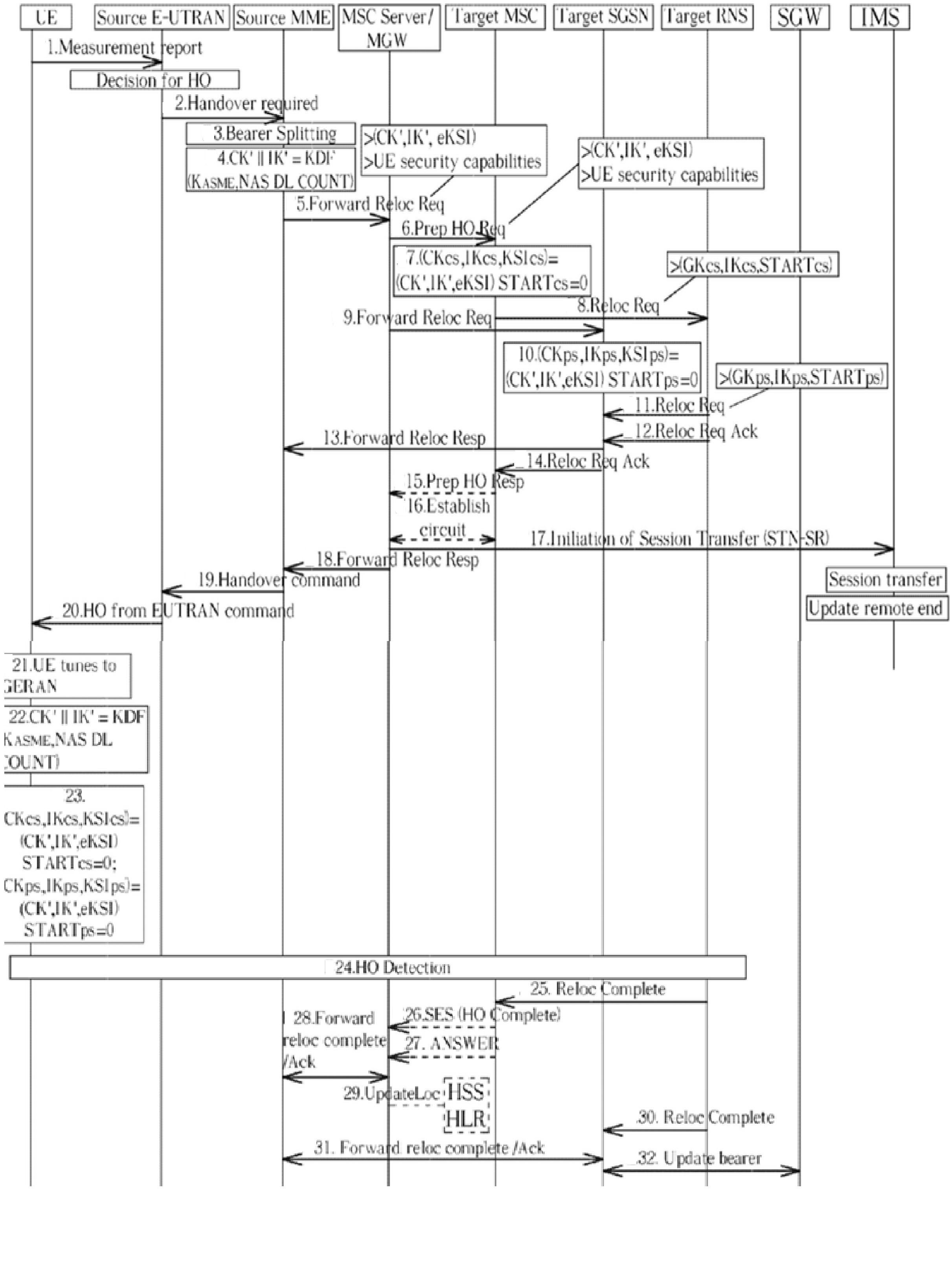


Figure 32. SRVCC Handover from E-UTRAN to UTRAN with PSHO support (Wu 2010).

of the MM Context.

7: The target MSC sets CK_{CS} to CK' , IK_{CS} to IK' , KSI_{CS} to eKSI and $START_{CS}$ to 0.

8: The target MSC requests resource allocation for the CS relocation by sending a *Relocation Request* message along with new set key values (CK_{CS}, IK_{CS}, $START_{CS}$) to the target RNS.

9: The MME sends a *Forward Relocation Request* message including the MM Context to the target SGSN. The *Forward Relocation Request* message has only non-voice component information.

10: The target SGSN sets its CK_{PS} to received CK', IK_{PS} to received IK', KSI_{PS} to eKSI received and $START_{PS}$ to 0.

11: The target SGSN requests resource allocation for the PS relocation by sending a *Relocation Request* message along with (CK_{PS}, IK_{PS}, $START_{PS}$) to the target RNS.

12: The target RNS acknowledges the prepared PS relocation by sending a *Relocation Request Acknowledge* message to the target SGSN.

13: The target SGSN sends a *Forward Relocation Response* message to the source MME.

14: The target RNS acknowledges the prepared CS relocation by sending a *Relocation Request Acknowledge* message to the target MSC.

15: The target MSC sends a *Prepare Handover Response* message to the MSC Server.
16: A circuit connection is established between the target MSC and the MGW (associated with the MSC Server).

17: The MSC Server starts a Session Transfer by sending an STN-SR message to the IMS. Hence the downlink flow of voice packets is switched towards a CS access leg.

18: The MSC Server sends a *Forward Relocation Response* message to the source MME.

19: The source MME synchronizes the PS and CS prepared relocations and sends a *Handover Command* message including a NAS DL COUNT to the source E-UTRAN.

20: The source E-UTRAN sends a Handover from E-UTRAN Command message to the UE.

21: The UE tunes to a frequency spectrum of the UTRAN system.
22: The UE derives a CK' and an IK' from its K_{ASME} and the received NAS DL COUNT with the KDF.

23: The UE sets both its (CK_{PS}, IK_{PS}, KSI_{PS}) and (CK_{CS}, IK_{CS}, KSI_{CS}) to the (CK', IK', eKSI), and sets both its $START_{PS}$ and $START_{CS}$ to 0.

24: The UE performs handover detection at the target RNS.

Steps in **Figure 32**, from 25 to 29 are used for completing the CS relocation, and steps from 30 to 32 are used for completing the PS relocation. From step 9 to 11 (in the same figure), the source MME starts relocation of the remaining non-voice PS bearers.

(Wu 2010.)

Scenario 3: SRVCC handover from E-UTRAN to GERAN with DTM support.

Refering **Figure 33**, during SRVCC handover from E-UTRAN to GERAN, the steps are almost the same as the steps of the SRVCC handover from E-UTRAN to UTRAN in **Figure 32**. Only the security content is different. Such as, the target MSC derives a GSM ciphering key Kc from the (CK', IK') with a conversion function c3 in **Figure 33: Step7**. The target MSC requests resource allocation for the CS relocation by sending a Relocation Request message including the GSM ciphering key Kc to the target BSS in **Figure 33:Step 8**. The target SGSN derives a GPRS ciphering key Kc from the (CK', IK') with the conversion function c3 in **Figure 33:Step10** compared. The UE tunes to a frequency spectrum of the GERAN system in **Figure 33:Step21**. The UE derives its own GPRS/GSM ciphering keys Kc from the (CK', IK') with the conversion function c3 in **Figure 33:Step23**.

(Wu 2010.)

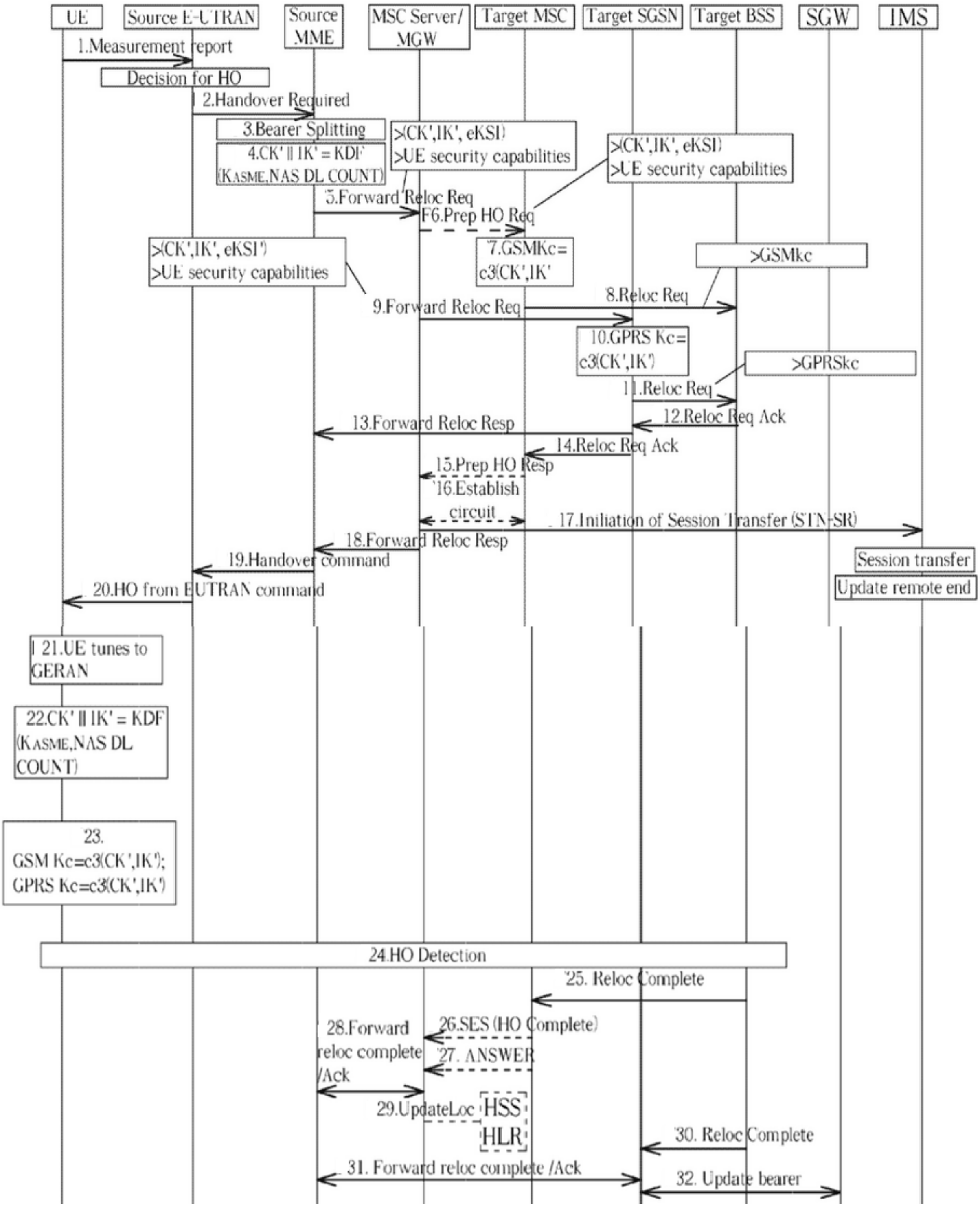


Figure 33. SRVCC handover from E-UTRAN to GERAN with DTM support (Wu 2010).

5.3.2. Integrity and Confidentiality Algorithms for LTE and UMTS

We have seen that how integrity, ciphering keys and KSI are being derived and exchanged during the SRVCC handover in different scenario. In case of IRATs handover, if source network is LTE and target network is UMTS/GSM then until handover trigger, LTE keys and their ciphering and integrity algorithms are used i.e. EIA and EEA. During the handover the target RAT network keys are generated by LTE NAS at UE and CN, and transferred to the target network's RRC at UE and at network side. At the target end, RNC selects UEA and UIA algorithms for ciphering and integrity in case of UMTS. Following algorithms are mentioned below for:

UMTS Integrity: UIA1 (Kasumi), UIA2 (SNOW 3G)
LTE Integrity: EIA1 (SNOW 3G), EIA2 ,5(AES), EIA3 (ZUC)
UMTS Ciphering: UEA0, UEA1 (Kasumi), UEA2 (SNOW 3G)
LTE Ciphering: EEA0, EEA1 (SNOW 3G), EEA2 (AES), EEA3 (ZUC)

In experimental work, the operating system is Ubuntu Linux and coding language is python. To verify the test data sets, CryptoMobile toolkit has been implemented from python 2.6 as wrapper around 3G and LTE encryption and integrity protection algorithms and compiled version of C source codes (provided by 3GPP, ETSI, GSMA, NIST) as .so files have been used. Test data sets are supposed to be verified according to flow chart (see **Figure 34**).

5.3.2.1. Input parameters for Integrity & Confidentiality Algorithms

For understanding of these integrity and ciphering algorithms, we can recall the core concept of stream and block ciphering from sections 3.6.1. and 3.6.2. Because, Kasumi and AES are block cipher while SNOW 3G and ZUC are stream cipher.

UMTS's integrity and confidentiality algorithms have been clearly explained in sections 4.3.3.2 and 4.3.3. But following is just quick reviw of input parameters for UMTS algorithms.

UEA2 – UMTS Encryption Algorithm: The input parameters are COUNT-C is frame dependent on input COUNTC[0]…COUNT-C[31] with 32 –bits length, BEARER is a bearer identity BEARER[0]…BEARER[4] with 5-bits length, DIRECTION is a direction of transmission DIRECTION[0] with 1-bit length, CK is Confidentiality key CK[0]….CK[127] with 128-bit length, LENGTH is the number of bits to be encrypted/decrypted and IBS is input bit stream IBS[0]….IBS[LENGTH-1] with LENGTH-bits longer. OBS is an output bit stream OBS[0]….OBS[LENGTH-1] with LENGTH-bits longer.

Initialization: Keystream generator is initialization with the key and initialization variables before the generation of keystream bits. Where all variables are 32-bits longer and are presented with the MSB on the left hand side and the LSB on the right hand side.

K3 = CK[0] || CK[1] || CK[2] || … || CK[31]

K2 = CK[32] || CK[33] || CK[34] || … || CK[63]

K1 = CK[64] || CK[65] || CK[66] || … || CK[95]

K0 = CK[96] || CK[97] || CK[98] || … || CK[127]

IV3 = COUNT-C[0] || COUNT-C[1] || COUNT-C[2] || … || COUNT-C[31]

IV2 = BEARER[0] || BEARER[1] || … || BEARER[4] || DIRECTION[0] || 0 || … || 0

IV1 = COUNT-C[0] || COUNT-C[1] || COUNT-C[2] || … || COUNT-C[31]

IV0 = BEARER[0] || BEARER[1] || … || BEARER[4] || DIRECTION[0] || 0 || … || 0

UIA2 – UMTS Integrity algorithm: The input parameters are COUNT-I is frame dependent on input COUNT-I[0]…COUNT-I[31] with 32-bits, FRESH is random number FRESH[0]…FRESH[31] with 32-bits, DIRECTION is a direction of transmission DIRECTION[0] with 1-bit, IK is integrity key IK[0]…IK[127] with 128-bits, LENGTH is the number of bits to be ‘MAC’d with 64-bits, MESSAGE is an input bit stream with LENGTH-bits. MAC-I is a message authentication code MAC-I[0]…MAC-I[31] with 32-bits.

Initialization:

K_3 = IK[0] || IK[1] || IK[2] || … || IK[31]

K_2 = IK[32] || IK[33] || IK[34] || … || IK[63]

K_1 = IK[64] || IK[65] || IK[66] || … || IK[95]

K_0 = IK[96] || IK[97] || IK[98] || … || IK[127]

IV_3 = COUNT-I[0] || COUNT-I[1] || COUNT-I[2] || … || COUNT-I[31]

IV_2 = FRESH[0] || FRESH[1] || FRESH[2] || … || FRESH[31]

IV_1 = DIRECTION[0] ⊕ COUNT-I[0] || COUNT-I[1] || COUNT-I[2] || … || COUNT-I[31]

IV_0 = FRESH[0] || FRESH[1] || … || FRESH[15] || FRESH[16] ⊕ DIRECTION[0] || FRESH[17] || … || FRESH[31]

(ETSI/SAGE V 2.1 2009.)

EEA – EPS Encryption algorithm: The input parameters to the ciphering algorithm are KEY is a cipher key with 128-bits, COUNT is with 32-bits, BEARER is a bearer identity with 5-bits, DIRECTION is the direction of the transmission with 1-bit, and LENGTH is the length of the keystream required. The DIRECTION bit shall be 0 for uplink and 1 for downlink.

EIA – EPS Integrity Algorithm: The input parameters are KEY is a integrity key with 128-bits, COUNT with 32-bits, BEARER is a bearer identity with 5-bits, DIRECTION is a direction of the transmission with 1-bit, and MESSAGE is the message itself with LENGTH-bits. The DIRECTION bit shall be 0 for uplink and 1 for downlink.

Based upon these input parameters the sender computes a 32-bit message authentication code (MAC-I/NAS-MAC) by using the integrity algorithm EIA. The MAC is then concatenated to the message when sent. The receiver computes the expected MAC (XMAC-I/XNAS-MAC) in the same way and verifies the data integrity of the message by comparing it to the received MAC-I/NAS-MAC. The stream cipher algorithm ZUC with an internal state of 560 bits is initialized from a 128-bit cipher key and a 128-bit initialization vector. (ETSI/SAGE V 2.0 2011.)

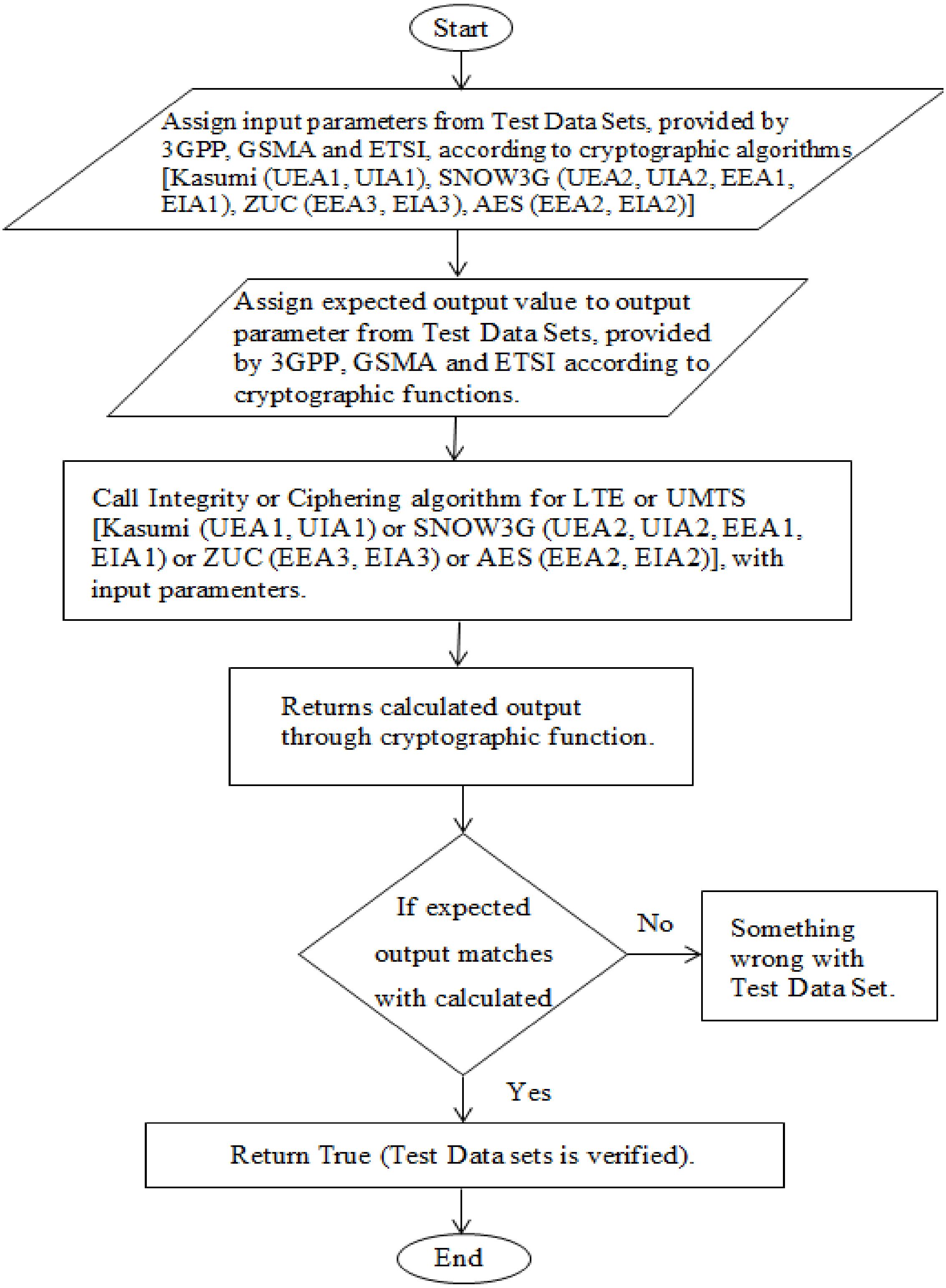

Start
Assign input parameters from Test Data Sets, provided by 3GPP, GSMA and ETSI, according to cryptographic algorithms [Kasumi (UEA1, UIA1), SNOW3G (UEA2, UIA2, EEA1, EIA1), ZUC (EEA3, EIA3), AES (EEA2, EIA2)]
Assign expected output value to output parameter from Test Data Sets, provided by 3GPP, GSMA and ETSI according to cryptographic functions.
Call Integrity or Ciphering algorithm for LTE or UMTS [Kasumi (UEA1, UIA1) or SNOW3G (UEA2, UIA2, EEA1, EIA1) or ZUC (EEA3, EIA3) or AES (EEA2, EIA2)], with input paramenters.
Returns calculated output through cryptographic function.
If expected output matches with calculated
No
Something wrong with Test Data Set.
Yes
Return True (Test Data sets is verified).
End

Figure 34. Flow Chart for Test Data Sets Verification.

5.3.2.2. Verification of Test Data Sets According to 3GPP Standards

All test data sets have been taken from 3GPP standards published in 3GPP technical specification, GSMA and ETSI/SAGE. Please see 3GPP TS 35.203, ETSI/SAGE V1.1 and 3GPP TS 33.401 for test data sets.

All input parameters are in hexadecimal format for each test case and hardcoded inside the testing code. Ciphering and integrity keys are 128-bits longer.

All test data sets against the Kasumi, Snow 3G, ZUC and AES algorithms have been executed by the test code. And it can be clearly seen in **Figure 35** that, the result is "True" as an output according to flow chart, which means all test data sets have been *verified.*

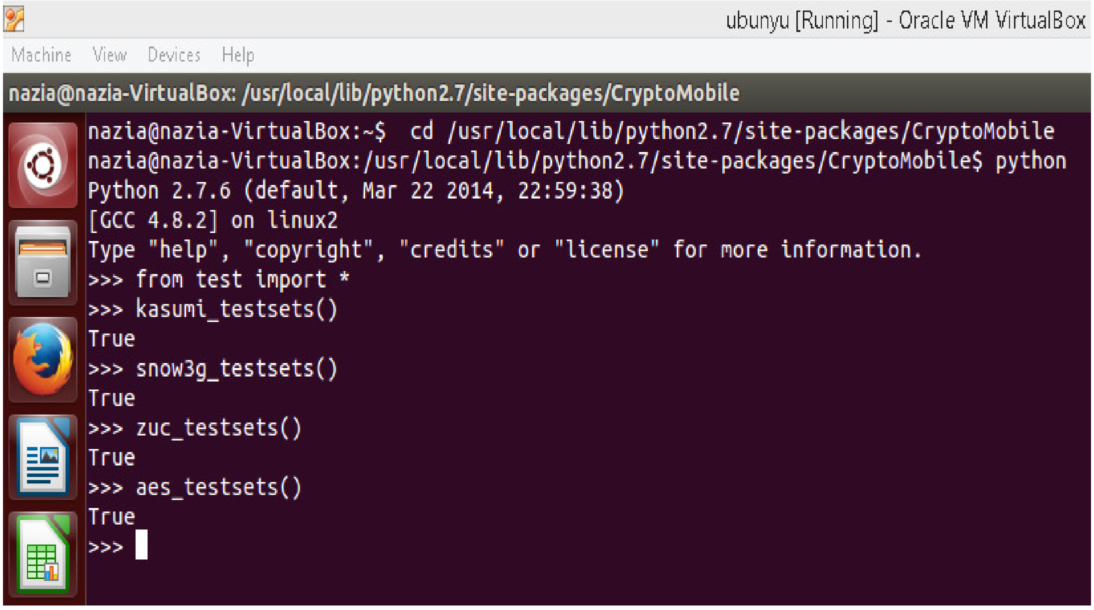
Verification of each data sets separately:

4 test data sets for kasumi and 5 test data sets for kasumi F8 and 5 test data sets for Kasumi F9, have been taken from 3GPP TS 35.203 V11.0.0 Release 11. After executing each sets of test data the result is "True" as an out put (see **Figure 36**). It means that these test data sets have been *verified* according to the flow chart.

From **Figure 37.a**, 4 test data sets for SNOW 3G, 5 test data sets for SNOW 3G F8 & F9 each, 6 test data sets for SNOW 3G EIA1 have been taken from ETSI/SAGE V 1.1 (2012). These data sets have been *verified* after execution of code same as above.

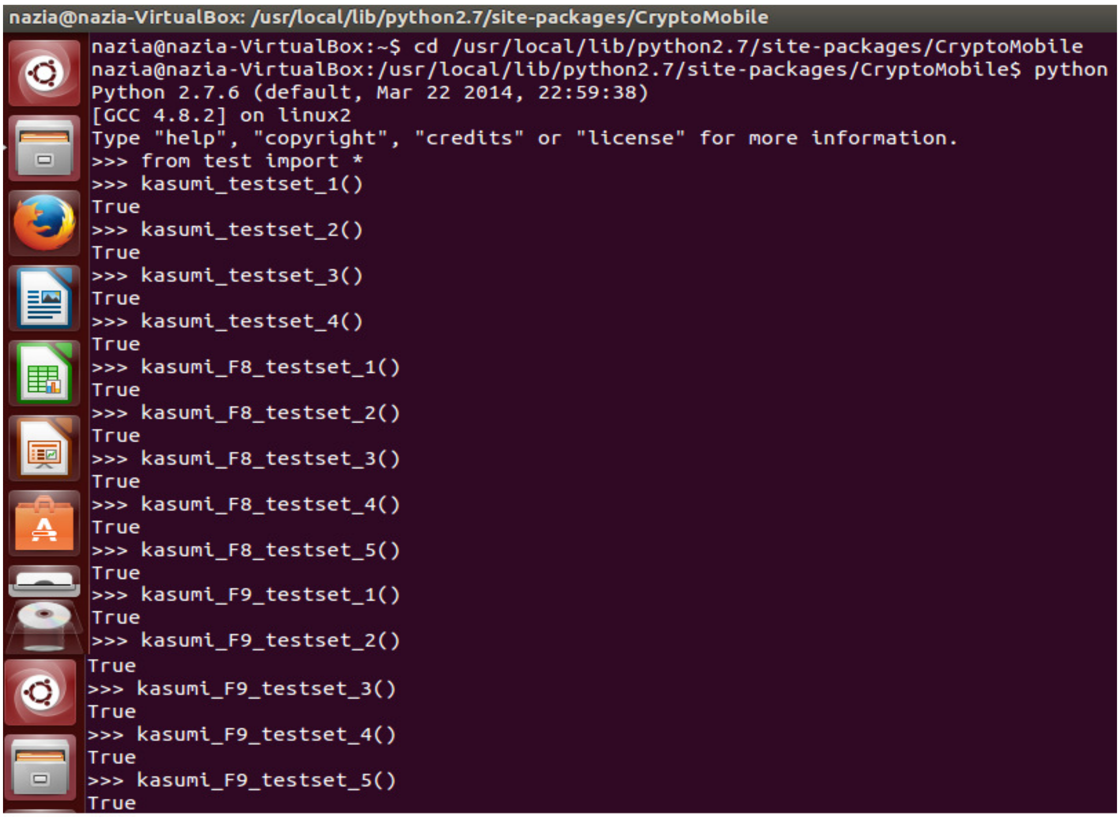
From **Figure 37.b**, 4 test data sets for ZUC, 5 test data sets for ZUC EEA3 and 5 test data sets for ZUC EIA3 have been taken from ETSI/SAGE V 1.1 (2011). These test data sets have been *verified* after execution the code as early mentioned case.

Figure 37.c, finally 6 test data sets for AES EEA2 and 8 test data sets for AES EIA2 have been taken from 3GPP TS 33.401 V8.6.0 Release 8. These data sets have been *verified* after execution of testing code.


ubunyu [Running] - Oracle VM VirtualBox
Machine View Devices Help
nazia@nazia-VirtualBox: /usr/local/lib/python2.7/site-packages/CryptoMobile

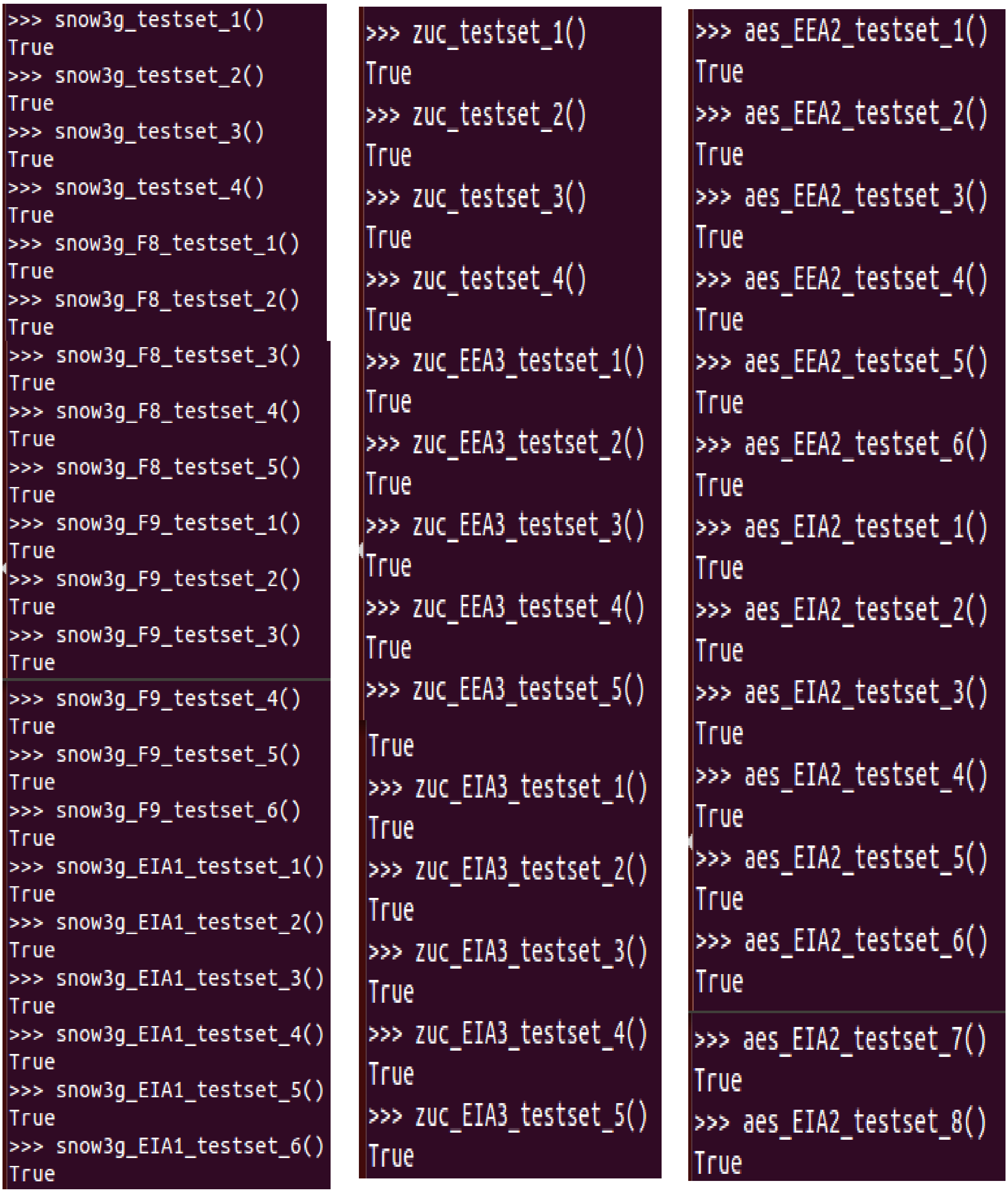
```
nazia@nazia-VirtualBox:~$  cd /usr/local/lib/python2.7/site-packages/CryptoMobile
nazia@nazia-VirtualBox:/usr/local/lib/python2.7/site-packages/CryptoMobile$ python
Python 2.7.6 (default, Mar 22 2014, 22:59:38)
[GCC 4.8.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from test import *
>>> kasumi_testsets()
True
>>> snow3g_testsets()
True
>>> zuc_testsets()
True
>>> aes_testsets()
True
>>>
```

Figure 35. Verification of Test Data Sets for Kasumi, Snow 3G, ZUC & AES.


nazia@nazia-VirtualBox: /usr/local/lib/python2.7/site-packages/CryptoMobile

```
nazia@nazia-VirtualBox:~$ cd /usr/local/lib/python2.7/site-packages/CryptoMobile
nazia@nazia-VirtualBox:/usr/local/lib/python2.7/site-packages/CryptoMobile$ python
Python 2.7.6 (default, Mar 22 2014, 22:59:38)
[GCC 4.8.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from test import *
>>> kasumi_testset_1()
True
>>> kasumi_testset_2()
True
>>> kasumi_testset_3()
True
>>> kasumi_testset_4()
True
>>> kasumi_F8_testset_1()
True
>>> kasumi_F8_testset_2()
True
>>> kasumi_F8_testset_3()
True
>>> kasumi_F8_testset_4()
True
>>> kasumi_F8_testset_5()
True
>>> kasumi_F9_testset_1()
True
>>> kasumi_F9_testset_2()
True
>>> kasumi_F9_testset_3()
True
>>> kasumi_F9_testset_4()
True
>>> kasumi_F9_testset_5()
True
```

Figure 36. Verification of Test Data Sets for Kasumi (F8 & F9).



```
>>> snow3g_testset_1()
True
>>> snow3g_testset_2()
True
>>> snow3g_testset_3()
True
>>> snow3g_testset_4()
True
>>> snow3g_F8_testset_1()
True
>>> snow3g_F8_testset_2()
True
>>> snow3g_F8_testset_3()
True
>>> snow3g_F8_testset_4()
True
>>> snow3g_F8_testset_5()
True
>>> snow3g_F9_testset_1()
True
>>> snow3g_F9_testset_2()
True
>>> snow3g_F9_testset_3()
True
>>> snow3g_F9_testset_4()
True
>>> snow3g_F9_testset_5()
True
>>> snow3g_F9_testset_6()
True
>>> snow3g_EIA1_testset_1()
True
>>> snow3g_EIA1_testset_2()
True
>>> snow3g_EIA1_testset_3()
True
>>> snow3g_EIA1_testset_4()
True
>>> snow3g_EIA1_testset_5()
True
>>> snow3g_EIA1_testset_6()
True
```

```
>>> zuc_testset_1()
True
>>> zuc_testset_2()
True
>>> zuc_testset_3()
True
>>> zuc_testset_4()
True
>>> zuc_EEA3_testset_1()
True
>>> zuc_EEA3_testset_2()
True
>>> zuc_EEA3_testset_3()
True
>>> zuc_EEA3_testset_4()
True
>>> zuc_EEA3_testset_5()
True
>>> zuc_EIA3_testset_1()
True
>>> zuc_EIA3_testset_2()
True
>>> zuc_EIA3_testset_3()
True
>>> zuc_EIA3_testset_4()
True
>>> zuc_EIA3_testset_5()
True
```

```
>>> aes_EEA2_testset_1()
True
>>> aes_EEA2_testset_2()
True
>>> aes_EEA2_testset_3()
True
>>> aes_EEA2_testset_4()
True
>>> aes_EEA2_testset_5()
True
>>> aes_EEA2_testset_6()
True
>>> aes_EIA2_testset_1()
True
>>> aes_EIA2_testset_2()
True
>>> aes_EIA2_testset_3()
True
>>> aes_EIA2_testset_4()
True
>>> aes_EIA2_testset_5()
True
>>> aes_EIA2_testset_6()
True
>>> aes_EIA2_testset_7()
True
>>> aes_EIA2_testset_8()
True
```

Figure 37. Verification of Test Data Sets

a. For SNOW 3G (F8, F9 & EIA1).

b. For ZUC (EEA3 & EIA3).

c. For EAS (EEA2 & EIA2).

5.4. SRVCC Emergency Call

3GPP Release 9 has introduced the SRVCC support for emergency calls that are anchored in the IMS core network. It must be supported in SRVCC where IMS emergency calls are used over IMS VoIP capable radio coverage and afterward is attended with the CS radio access. The *Emergency Access Transfer Function* (EATF) is a logical function required in the *Visited Public Land Mobile Network* (VPLMN) in addition to the functions needed for SRVCC and IMS emergency calls. The MSC uses the *Mw* interface to the I-CSCF and includes the equipment identifier into the session transfer request; the equipment identified is used by the EATF to correlate the call legs (see **Figure 38**). SRVCC for emergency calls does not make use of the *Access Transfer Control Function* (ATCF) and *Access Transfer Gateway* (ATGW). The MSC can also use the *ISDN User Part* (ISUP) interface to a *Media Gateway Control Function* (MGCF) and then the *Mg* interface is used between the MGCF and the I-CSCF. It is assumed that if ISUP is used, the ISUP extension of carrying the IMEI to the MGCF is supported. Support of SRVCC for emergency calls requires support in MME, MSC Server, Emergency CSCF (E-CSCF) and EATF. (GSMA IR.64 2012.)

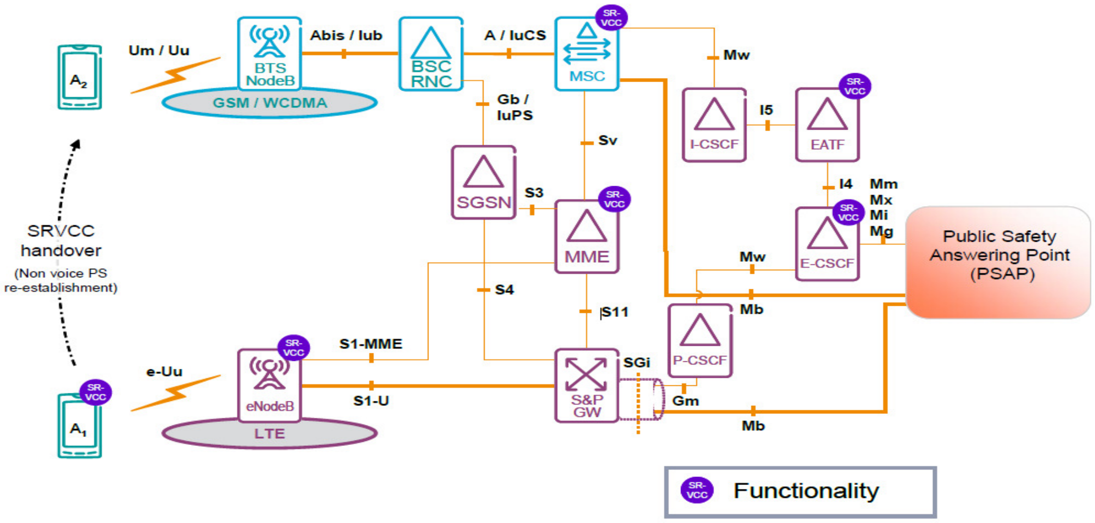


Figure 38. SRVCC For Emergency Call (GSMA IR.64 2012).

5.4.1. Security in SRVCC Emergency Call

During the IMS emergency calls, the session data of all calls is stored by the application server that is responsible for the VCC functionality until the completion of emergency session. It is obligatory to re-generate the security parameters during SRVCC between E-UTRAN to UTRAN/GERAN. In case of mobility from E-UTRAN to UTRAN, the UTRAN ciphering and integrity protection keys are derived from the EPS security key, so there is no need to send confidential security parameters over the radio interface as a part of session transfer mechanism. If the authentication has been omitted in E-UTRAN because of absence of a valid USIM, "then instead of seeding the key derivation with locally created keys for a null algorithm, the already existing UTRAN and GERAN practice to omit the security procedure can be used" (Schulzrinne 2013).

6. CONCLUSION AND FUTURE WORK

Objective of this thesis is to identify and review security measures in cellular, mobile network. The attention is paid to SRVCC procedure along with test data sets verification against the integrity and ciphering (UIA, UEA, EIA and EIA) algorithms for UMTS and LTE network.

Therefore, the following is presented in the thesis: basic idea of architecture, operation and evolution of a cellular network; basic concept of security and an evolution of the security measures employed in the cellular networks ranging from 2G to 4G. Also the thesis elaborates on the architecture of mobile networks, identification of possible threats, vulnerabilities, risks and attacks against the mobile networks. Moreover counter measures for the latter, in terms of security architecture of mobile networks including authentication, confidentiality and integrity, to protect the whole system are concrete pillars of security infrastructure.

When a single radio UE accessing IMS-anchored voice call services moves from the LTE network to the circuit switched domain, the SRVCC service for LTE comes into the picture. It is capable of transmitting/receiving on one of these access networks only, at a given time. SRVCC removes the need for a UE to have multiple RAT capability. In this thesis, the review of the scenarios for SRVCC triggered handover is presented, and it is concluded that the security configuration of each system can be stored in the USIM or the ME of the UE. The UE can transmit a handover complete message to activate ciphering/integrity protection with the updated security configuration after the handover command is received. Along with this test data sets have been verified for Kasumi, SNOW 3G, ZUC and AES cryptographic algorithms for LTE's and UMTS's integrity and confidentiality provided by authentic organization with 128-bits ciphering and integrity keys.

For future work test data sets can be tested with 256-bits ciphering and integrity keys. Moreover, security measures for SRVCC procedure have been considered only for voice component, in future it might be reviewed for *Single Radio Video Call Continuity* (vSRVCC) that is a network domain handover technology with TV phone service. Security assurance methodology for 3GPP network is also an interesting research topic in security context. Especially security measures during interworking and interoperability between LTE and non-3GPP wireless mobile networks.

REFERENCES

3GPP TS 25.331 V11.4.0 Release 11.Technical Specification Group RadioAccess Network; Radio Resource Control (RRC): Protocol Specification.

3GPP TS 29.002 V3.20.0 Release 1999. Technical Specification Group Core Network; Mobile Application Part (MAP) specification.

3GPP TS 33.203 V8.5.0 Release 8. 3G Security: Access Security for IP-Based Service.

3GPP TS 33.401 V8.6.0 Release 8. Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture.

3GPP TS 33.102 V9.2.0 Release 9. 3G Security: Security architecture.

3GPP TS 33.102 V9.4.0 Release 9. 3G Security: Security architecture.

3GPP TS 33.210 V9.0.0 Release 9. 3G Security: 3G Security; Network Domain Security; IP network layer security.

3GPP TS 35.201 V11.0.0 Release 11. Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the 3GPP confidentialityand integrity algorithms; Document 1: f8 and f9 specification

3GPP TS 35.202 V11.0.0 Release 11.Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification

3GPP TS 35.203 V11.0.0 Release 11. Universal Mobile Telecommunications System (UMTS); LTE ;3G Security;Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data

3GPP TS 35.204 V11.0.0 Release 11.Universal Mobile Telecommunications

System (UMTS); LTE; 3G Security; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data

3GPP TS 33.401 V12 Release 12. 3GPP System Architecture Evolution (SAE); Security Architecture.

3GGP TS 33.402 V8.2.1 Release 8. 3G System Architecture Evolution (SAE): Security aspect of non 3GPP accesses.

3GPP TSG SA WG3 Security-S3#20 (2001). ISIM/USIM Independence [online]. [cited 2 Apr. 2014]. Available from World Wide Web < URL: http://www.3gpp.org /ftp/tsg_sa/wg3_security/TSGS3_20_Sydney/Docs/PDF/S3-010468.pdf >

Abid, Muslim, Selo Sulistyo & Warsun Najib (2002). UMTS Security: Security in Core Network and UTRAN [online]. [cited 15 Mar. 2014]. Available from World Wide Web <URL :http://www.oocities.org/warsunnajib/Warsun2file/SecuritSolutioiUMTS _Report.pdf >

Aono, Hiroshi & Alf Zugenmaier (2009). Security Technology for SAE/LTE [online]. NTT DOCOMO Technical Journal Vol. 11 No.3 [cited 25 Mar.2014]. Available from World Wide Web < URL: https://www.nttdocomo.co.jp/english/ >

Bais, Abdul, Peter Palensky & Walter T. Penzhorn (2006). Evaluation of UMTS security architecture and services.©IEEE. ISSN: 1-4244-9701-0

Bikos, Anastasios N. & Nicolas Sklavos (2013). LTE/SAE Security Issues on 4G Wireless Networks [online]. ©IEEE Security & Privacy,Volume: 1, Issue: 2. [cited 24 Mar. 2014]. ISSN: 1540-7993. Available from World Wide Web < URL: http://www. computer.org/security>

Boman, Krister, Giinther Horn, Peter Howard & Valtteri Niemi (2002). UMTS security [online]. ©IEEE [cited 21 Mar. 2014]. Available from World Wide Web < URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01088436 >

Bocan, Valer & Vladimir Cretu (2006). Threats and Countermeasures in GSM Networks [online]. ©ACADEMY, Journal of Networks, Vol. 1, No.6. [cited 4 Mar. 2014]. Available from World Wide Web <URL: http://ojs.academypublisher.com /index.php/jnw/article/viewFile/010618/655 >

Brookson, Charles (2001). GPRS Security [online]. [cited 5 Mar. 2014]. Available from Internet: < URL: http://www.brookson.com/gsm/gprs.pdf >

Cao, Jin, Hui Li, Maode Ma,Yueyu Zhang & Zhenxing Luo (2013). A Survey on Security Aspects for LTE and LTE-A Networks. ©IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1. ISSN: 1553-877X.

Choi, Hyoung-Kee & Chan-Kyu Han (2014). Security Analysis of Handover Key Management in 4G LTE/SAE Networks.IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 2. ©IEEE CS, CASS, ComSoc, IES, & SPS.

Douligeris, Christos & Panayiotis Kotzanikolaou (2006). Telecommunication Systems and Technlogies-Vol. II- Network Security, ©Encyclopedia of Life Support Systems (EOLSS). ISBN: 978-1-84826-001-6.

Egners, André, Enno Rey, Hendrik Schmidt, Peter Schneider & Sascha Wessel (2012). Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals [online]. D5.1(II)-1.0, ©ASMONIA Consortium. [cited 27 Feb. 2014]. Available from World Wide Web < URL: http://www.asmonia.de/deliverables/ D5.1_ II_ThreatAndRiskAnalysisMobileCommunicationNetworksAndTerminals.pdf >

Elouafiq, Ali (2012). Authentication and Encryption in GSM and 3G/UMTS-An

Emphasison Protocols and Algorithms [online]. [cited 6 Mar. 2014]. Available from World Wide Web < URL: http://arxiv.org/find/cs/1/au:+Elouafiq_A/0/1/0/all/0/1 >

ETSI/SAGE V2.1 (2009). Specification of the 3GPPConfidentiality and Integrity Algorithms UEA2 & UIA2. Document 1: UEA2 and UIA2 Specification.

ETSI/SAGE V1.1 (2006). Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification.

ETSI/SAGE V1.1 (2012). Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 3: Implementors' Test Data.

ETSI/SAGE V1.0 (2006). Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 4: Design Conformance Test Data.

ETSI/SAGE V1.1 (2006). Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 5: Design and Evaluation Report.

ETSI/SAGE V1.7 (2011). Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 1: 128-EEA3 and 128-EIA3 Specification.

ETSI/SAGE V1.1 (2011). Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3.Document 3: Implementor's Test Data.

ETSI/SAGE V2.0 (2011). Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3.Document 4: Design and Evaluation Report.

Forsberg, Dan, Günther Horn, Wolf-Dietrich Moeller & Valtteri Niemi (2010). LTE Security. ©John Wiley & Sons, Inc. ISBN: 978-0-470-66103-1.

Fundamental Security Concept (2013) [online]. [cited 17 Feb. 2014]. Available from

World Wide Web <URL: http://cryptome.org/2013/09/infosecurity-cert.pdf >

Gardezi, Ali I. (2006). Security in Wireless Cellular Networks [online]. [cited 10 Feb 2014]. Available from World Wide Web < URL: http://www.cse.wustl.edu/~jain/cse574-06/ftp/cellular_security.pdf >

Gilbert, Henri. Design and Analysis of Cryptographic Algorithms for Mobile Communication Systems from ©orange Labs.

Godin , Philippe & Palat, Sudeep (2009). LTE - The UMTS Long Term Evolution: From Theory to Practice. Edited: Sesia, Stefania, Toufik, Issam & Baker, Matthew (Alcatel-Lucent's 3GPP standardization team), Print ISBN: 9780470697160. Electronic ISBN: 9780470742891.

Gupta, Asheesh (2013). Generations of Wireless Network : 1G, 2G, 3G & 4G - Mobile Computing [online]. ©2014 Google [cited 10 Feb. 2014]. Available from World Wide Web: < URL: https://sites.google.com/site/nexttowirelessnews/generations-of-wireless-network-1g-2g-3g-4g---mobile-computing >

Huovinen, Lasse (2007). Authentication and Security in GPRS Environment: An Overview [online]. [cited 8 Mar. 2014]. Available from World Wide Web < URL: http://www.tml.tkk.fi/Opinnot/Tik-10.501/1998/papers/11gprs_access/gprs _access.html>

Huynh, Tuan & Hoang Nguyen (2003). Overview of GSM and GSM Security. Department of Electrical Engineering and Computer Science, Oregon State University, USA.

InfoSec Reading Room (2001). The GSM Standard (An overview of its security) [online]. ©SANS Institute [cited 1 Mar. 2014]. Available from World Wide Web < URL: http://www.sans.org/reading-room>

IBM (2014). IP Security (IPSec) Protocols [online]. [cited 20 Feb. 2014]. iSeries Information Center, Version 5 Release 3. Available from World Wide Web < URL: https://publib.boulder.ibm.com/infocenter/iseries/v5r3/topic/rzaja/rzajaipsec.htm >

Katz, Jonathan (2004). Advanced Topics on Cryptography [online]. [cited 10 Feb. 2014]. Available from World Wide Web < URL: http://www.cs.umd.edu/~jkatz/ gradcrypto2/NOTES/lecture4.pdf >

Khan, Wilayat & Habib Ullah (2010). Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography [online]. [cited 10 Mar. 2014]. ISSN: 1694-0784. Available from World Wide Web < URL: http://www.IJCSI.org >

LinYing, Li & Song WenYuan (2012). Forward Handover for Voice Call Continuity. Next Generation Mobile Applications, Services and Technologies (NGMAST), International Conference.Paris, France. © IEEE. ISSN: 2161-2889.

Ma, Maode (2012). Security Investigation in 4G LTE Wireless Networks. ©IEEE GLOBECOM Tutorial Program, T10.

Margrave, David. GSM Security and Encryption.George Mason University [online]. [cited 1 Mar. 2014]. Available from World Wide Web< URL: http://www. hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html >

Martin, Tobias, Stefan Pütz & Roland Schmitz (2001). SecurityMechanisms in UMTS [online]. DuD 25 X based on VIS200 [cited 24 February. 2014]. Available from World Wide Web < URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi =10.1 .1.84.6356&rep=rep1&type=pdf >

Mazurkevich D.O., V.G.Orlov (2011). Evolution of Security Systems in Different Generations of Cellular Networks [online]. Moscow Technical University of Communication and Informatics (MTUCI), Russia [cited 9 April. 2014]. Available from World Wide Web < URL: http://www.media-publisher.ru/pdf/2011-1-eng/8.pdf >

Merakos, Lazaros & Christos Xenakis (2006). Vulnerabilities and Possible Attacks against the GPRS Backbone Network [online]. 1st International Workshop on Critical Information Infrastructures Security. Department of Informatics & Telecommunications, University of Athens, Greece [cited 20 Mar. 2014]. Available from World Wide Web < URL: http://critis06.lcc.uma.es/files/Vulnerabilities and Possible Attacks against the GPRS Backbone Network.pdf>

NetScreen Technologies Inc. (2002). GPRS Security Threats and Solutions [online]. [cited 16 Mar. 2014]. Available from World Wide Web < URL: http://www.netscreen.com>

Nilanka, G.V. (2011). Cellular Technologies and Security [online]. [cited 24 Feb. 2014]. Available from World Wide Web < URL: http://www.slideshare.net /nilankamora/cellular-technologies-and-security>

Nyberg, Kaisa (2004). Cryptographic Algorithms for UMTS [online]. © ECCOMAS [cited April 2014]. Available from World Wide Web < URL: http://www.tcs.hut.fi/Publications/knyberg/eccomas.pdf?origin=publication_detail >

Pagtzis, Theo (1999). Cellular Systems [online]. Department of Computer Science, University College London. © UCL [cited 10 Feb. 2014]. Available from World Wide Web < URL: http://www.cs.ucl.ac.uk/staff/t.pagtzis/wireless/gsm/cellular.html >

Paar, Christof & Jan Pelzl (2010). Understanding Cryptography. © Springer. XVIII, 372 p. ISBN: 978-3-642-04101-3.

Park,Yongsuk & Taejoon Park (2007). Survey of Security Threats on 4G Networks [online]. © IEEE [citet 26 April 2014]. Available from World Wide Web < URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04437813 >

Parsad, Anand R. (2011). 3GPP SAE/LTE Security. ©NEC Corporation. Presented at NIKSUN WWSMC, NJ, USA.

Paisal, Vaishali (2010). Seamless Voice over LTE. ©IEEE. 4th International Conference. Digital Object Identifier: 10.1109/IMSAA.2010.5729423.

Perez, David & Jose Pico (2011). A practical attack against GPRS/EDGE/ UMTS/ HSPA mobile data communications [online]. Black Hat-White Paper [cited 25 Mar. 2014]. Available from World Wide Web < URL: https://media.blackhat.com/ bh-dc-11/Perez-Pico/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-wp.pdf >

Purkhiabani, Masoumeh & Ahmad Salahi(2012). Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks [online]. International Journal of Information and Electronics Engineering (IJIEE), Vol. 2, No. 1 [cited Apr. 2014]. Available from World Wide Web < URL: http://www.ijiee.org/papers/57-C099.pdf >

Qualcomm (2012). VoLTE with SRVCC: The Second Phase of Voice Evolution for Mobile LTE Devices. Qualcomm Technologies, Inc. White Paper, collaboration with Ericsson.

Rumney, Moray (2008). LTE and the Evolution to 4G Wireless: Design and Measurement Challenges. 2nd Edition. ©John Wiley & Sons, Inc. ISBN: 978-1-119-96257-1.

Schulzrinne, Henning (2013). Internet Protocol-based Emergency Services. Editors: Hannes Tschofenig, Henning Schulzrinne . ©John Wiley & Sons, Ltd. 408 p. Print ISBN: 9780470689769, Electronic ISBN: 9781118652473.

Stallings, William (2010). Cryptography and Network Security: Principles and Practice. 5th Edition. ©Prentice Hall. 774 p. ISBN-13: 978-0-13-609704-4, ISBN-10: 0-13-609704-9 .

Stepanov, Max (2003). GSM Security Overview (Part 2) [online]. Hebrew University of Jerusalem [cited 4 Mar. 2014]. Available from World Wide Web < URL: http:// pt.slideshare.net/ Garry54/gsm-security-by-max-stephan >

Syben, Tim (2011). Introduction to Block Ciphers [online]. University of Bonn, Germany [cited 18 Feb. 2014]. Available from World Wide Web < URL: http:// cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/11ss/blockciphers/Talks/ Tim_Syben.pdf >

Tipper, David (2009). UMTS Overview [online]. University of Pittsburgh, USA [cited 25 Mar. 2014]. Available from World Wide Web < URL:http://www.pitt.edu/ ~dtipper/2720/2720_Slides12.pdf >

Tutorialspoint (2014). GPRS Architecture [online]. [cited 8 Mar. 2014]. Available from World Wide Web < URL: http://www.tutorialspoint.com/gprs/ gprs_architecture .htm >

Tutorialspoint (2014). LTE Network Architecture [online]. [cited 23 Mar. 2014]. Available from World Wide Web < URL: http://www.tutorialspoint.com/lte/lte_ network _architecture.htm >

UMTSWorld (2002). Overview of Universal Mobile Telecommunication System [online]. ©UMTSWorld.com [cited 6 Mar. 2014]. Available from World Wide Web < URL: http://www.umtsworld.com/technology/overview.htm#a3 >

UNT (2003). Information Security [online]. University of North Texas, USA [cited 16 Feb. 2014]. Available from World Wide Web < URL: https://security.untsystem.edu/ resources/networksecurity >

Wheeler, David A. (2004). Secure Programming for Linux and Unix HOWTO [online]. [cited 20 Feb. 2014]. Available from World Wide Web < URL: http://www.dwheeler .com/secure-programs/Secure-Programs-HOWTO/crypto.html >

Wu, Chih-Hsiang (2010). Method of Handling Handover Security Configurationand Related Communication Device.Taoyuan County, TW. IPC8 Class: AH04W3634FI. USPC Class: 455436. Patent application number: 20100130207.

Yang, Herong (2014). Cryptography Tutorials:Herong's Tutorial Examples [online]. [cited 20 Feb. 2014]. Available from World Wide Web < URL: http://www. herongyang .com/Cryptography/pdf.html >

Yang, Li (2014). Conventional Cryptography [online]. Department of Computer Science and Engineering, University of Tennessee, Chattanooga [cited 23 Feb. 2014]. Available from World Wide Web < URL: http://www.learningace.com/ doc/2560345/ 34dab7dc2bba4a9d32447cf79859aaca/02-utc-conventional-crypto >

Zimmermann, Phil (2000). An Introduction to Cryptography[online]. ©Network Associates, Inc. CA, USA [cited 10 Feb. 2014]. Available from FTP < ftp://ftp .pgpi. org /pub/pgp/6.5/docs/english/IntroToCrypto.pdf >