Evaluation of UICC-based IMS authentication schemes

This thesis is presented as part of Degree of Master of Science in Electrical Engineering with emphasis on Telecommunications

Blekinge Institute of Technology
School of Engineering
Department of Telecommunication systems

Submitted By: Muhammad Adeel Khan Jadoon
P-Number: 830731-7555

24\textsuperscript{th} March 2009

Supervisor: Charlott Eliasson
Department of Telecommunication Systems, Blekinge Institute of Technology, Sweden

Examiner: Markus Fiedler
Department of Telecommunication Systems, Blekinge Institute of Technology, Sweden
ABSTRACT

This thesis study involves evaluation of UICC based IMS authentication schemes. The schemes included in this study are IMS AKA, E-IMS AKA, One-Pass GPRS IMS authentication and Early IMS security. These schemes are evaluated on the basis of security, user friendliness and simplicity. Based on the analysis it is concluded that the IMS AKA which is the standardized authentication mechanism for IMS and embedded in ISIM is the most suitable authentication scheme for IMS, regardless of access network. However, the Early IMS authentication scheme is used only for GSM/GPRS network.
Acknowledgment

I would like to acknowledge and extend my heartfelt gratitude, to my thesis supervisor Charlott Eliasson at Department of Telecommunication Systems, Blekinge Tekniska Högskola (BTH), Sweden, for her support and encouragement which has made the completion of this thesis possible. Throughout my work with this thesis, I have received so much help from you. Thanks for catching my misunderstandings and unclear wordings and thereby greatly improving the quality of this report. Thanks also for all your ideas and suggestions; they have guided me to improve my technical and non-technical skills. This thesis would have been an uninspired struggling little piece of work without your help.

My greatest appreciation also goes, to my examiner Markus Fiedler at Blekinge Tekniska Högskola (BTH), for his advice, time and interest.

Finally, I thank my friends and family for supporting me throughout all my studies at BTH. Their love and affection didn’t make me feel that I am alone.

Karlskrona, 24th of March 24, 2009

Muhammad Adeel Khan Jadoon
Table of Contents

1 INTRODUCTION ................................................................................................. 11
  1.1 Thesis Objective ............................................................................................... 11
  1.2 Thesis Scope .................................................................................................... 11
  1.3 Thesis Outline .................................................................................................. 12
2 BACKGROUND .................................................................................................... 13
  2.1 Security ........................................................................................................... 13
  2.2 Authentication Process .................................................................................. 14
3 THE IMS ............................................................................................................ 16
  3.1 GSM to IMS .................................................................................................... 17
  3.2 Network Architecture ..................................................................................... 17
  3.3 IMS Core Network .......................................................................................... 18
    3.3.1 Home subscriber Server (HSS)................................................................. 18
    3.3.2 Call Session Control Function (CSCF) .................................................... 18
    3.3.3 Proxy CSCF (P-CSCF) ............................................................................ 18
    3.3.4 Interrogating CSCF (I-CSCF) ................................................................. 19
    3.3.5 Serving CSCF (S-CSCF) .......................................................................... 19
    3.3.6 Application Servers (AS) .......................................................................... 20
    3.3.7 IMS terminal ............................................................................................ 20
    3.3.7.1 IMS service identity module (ISIM).................................................... 20
  3.4 SIP in IMS ....................................................................................................... 22
  3.5 Why SIP .......................................................................................................... 22
4 AUTHENTICATION MECHANISM....................................................................... 23
  4.1 Authentication in GSM/GPRS ......................................................................... 23
    4.1.1 GSM/GPRS Subscriber Authentication Mechanism............................. 24
  4.2 Security Mechanism in UMTS ....................................................................... 25
    4.2.1 UMTS AUTHENTICATION .................................................................... 25
    4.2.2 AKA Prerequisites .................................................................................. 26
    4.2.3 UMTS AKA ............................................................................................. 26
  4.3 Authentication in IMS .................................................................................... 27
    4.3.1 Security architecture ................................................................................ 28
    4.3.2 Authentication Schemes in IMS .............................................................. 29
    4.3.2.1 UICC based Authentication Schemes ............................................... 30
5 IMS AUTHENTICATION SCHEMES .................................................................. 32
  5.1 Authentication using IMS AKA ....................................................................... 33
  5.2 ISIM Based Authentication ............................................................................ 33
    5.2.1 USIM based Authentication .................................................................. 36
  5.3 Early IMS Security .......................................................................................... 37
    5.3.1 Authentication Procedure ....................................................................... 39
  5.4 One Pass GPRS-IMS Authentication ............................................................ 42
  5.5 Evolutionary IMS AKA .................................................................................. 43
    5.5.1 Detailed procedure .................................................................................. 44
6 EVALUATION ..................................................................................................... 47
  6.1 Evaluation Based on Security ......................................................................... 47
Table of figures

FIGURE 3-1: IMS NETWORK ARCHITECTURE ................................................................. 19
FIGURE 3-2: IP MULTIMEDIA SERVICES IDENTITY MODULE ........................................ 21
FIGURE 4-1: UMTS AUTHENTICATION MECHANISM .................................................. 27
FIGURE 4-2: IMS SECURITY ARCHITECTURE .............................................................. 28
FIGURE 4-3: ACCESS AND NETWORK DOMAIN SECURITY ........................................... 29
FIGURE 5-1: IMS SECURITY FEATURES ......................................................................... 32
FIGURE 5-2: AV GENERATION AT NETWORK ................................................................. 34
FIGURE 5-3: AV GENERATION AT ISIM .......................................................................... 35
FIGURE 5-4: IMS AKA REGISTRATION/AUTHENTICATION SIGNALING FLOW .................. 36
FIGURE 5-5: EARLY IMS REGISTRATION/AUTHENTICATION SIGNALING FLOW ............. 41
FIGURE 5-6: ONE-PASS GPRS IMS REGISTRATION/AUTHENTICATION SIGNALING FLOW .......................................................... 43
FIGURE 5-7: E-IMS REGISTRATION/AUTHENTICATION SIGNALLING FLOW ..................... 45
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>AKA</td>
<td>Authentication and Key Agreement</td>
</tr>
<tr>
<td>AuC</td>
<td>Authentication Centre</td>
</tr>
<tr>
<td>CK</td>
<td>Confidentiality Key</td>
</tr>
<tr>
<td>CSCF</td>
<td>Call Session Control Function</td>
</tr>
<tr>
<td>E-IMS AKA</td>
<td>Evolutionary IMS AKA</td>
</tr>
<tr>
<td>FMC</td>
<td>Fixed Mobile Convergence</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber System</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IK</td>
<td>Integrity Key</td>
</tr>
<tr>
<td>IMPI</td>
<td>IMS Private User Identity</td>
</tr>
<tr>
<td>IMPU</td>
<td>IMS Public User Identity</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>ISIM</td>
<td>IP multimedia Subsystem Service Identity Module</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile Subscriber</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Subscriber Integrated Services Digital Network</td>
</tr>
<tr>
<td>RAND</td>
<td>Random Number</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SQN</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>TISPAN</td>
<td>Telecommunications and Internet converged Services and Protocols for Advance Networking</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>AV</td>
<td>Authentication Vector</td>
</tr>
</tbody>
</table>
1 Introduction
It is of utmost importance to protect the subscriber, the networks entities and the resources from illegitimate use and intruders that can harm or take advantage from the system illegally. To cater these security issues different security algorithms are implemented in every communication network in the access and network domain subsystem. IMS is a global and access independent IP architecture that provides various types of multimedia services to the end-users. Hence the security in the access and network domain part of IMS is very important.

The access domain security in IMS can have an extensive challenge as almost all types of communication networks are supported and almost every networks has its own method of access security i.e. authentication. Although the standardized authentication mechanism in IMS is based on the use of specific ISIM module, which is embedded in UICC and stores the identities, keys and algorithms for subscriber authentication to IMS services. There are different authentication schemes that can be employed in IMS service authentication and these can be categorized as SIM based and non SIM based

1.1 Thesis Objective
In this thesis work only UICC based authentication schemes that can be implemented in IMS will be evaluated. A detailed study of different UICC based authentication schemes will be carried out to study and generalize a single authentication mechanism for IMS.

There are different authentication mechanism based on UICC and in this regard the Authentication schemes like ISIM/USIM based IMS AKA, Evolutionary-IMS AKA, One-Pass GPRS IMS authentication and Early IMS security will be studied. Based on these studies the schemes will be evaluated in different aspect relating to security, user friendliness and simplicity and the result gathered from this evaluation will be used to generalize an IMS authentication mechanism which can be implemented in any device regardless of the type of device and access network supported.

1.2 Thesis Scope
The schemes to be evaluated include the ISIM based, USIM based and SIM based authentication mechanism. All these ISIM, USIM, SIM are the modules embedded in the UICC card. SIM is the module which is used for subscription and authentication tool for GSM/GPRS network. USIM is used for the same purposes like the SIM in UMTS network. ISIM was specifically developed for the IMS network and contains Subscription and Authentication/Registration data for IMS.

The UICC based authentication scheme is used for IMS authentication when the access network is defined by 3GPP, however with the slight
modifications in the UE or the access network, we can use this mechanism in almost any type of the fixed and wireless networks through which the IMS services are offered. However, the scope of the thesis work is limited by considering only the cellular networks in the access side.

1.3 Thesis Outline

Chapter 2 provides a description of security with an emphasis on the authentication including the authentication levels defined by NIST.

Cellular Networks
Chapter 3 describes the IMS architecture, network entities and reference points used between different network components. It also gives an overview of the protocols specifically used in authentication mechanism in IMS.

Chapter 4 gives a brief overview of authentication mechanism in communication networks. The chapter proceeds with the description of the authentication procedure in GSM/GPRS and UMTS. An overview of IMS security mechanism is also given.

Chapter 5 provides a detailed study of the authentication schemes based on UICC that can be implemented in IMS. The evaluation of these authentication schemes based on the different parameters can be found in chapter 6, followed by the chapter 7 which provides the detailed analysis of the schemes. Chapter 8 is the conclusion of the thesis and future research work is depicted in chapter 9.
2 Background

The condition or quality of being free from apprehension, anxiety, or care” is the definition of security defined in Webster dictionary. A secure communication network is a network in which user do not feel apprehension or anxiety while using the network resources. An important issue in the current telecom network is the security. As more sophisticated techniques to secure the networks increases, the tools and methods to attack the network also increases. Security is a concept, it is difficult to define but easy to understand what it is and what are the issues related to it. The security aspect principally concerns the behavior of the network as seen by the service providers and the networks operators.

2.1 Security

In Communication networks security is to protect the communicating entities and there communication. The typical classification of security is physical security and the information security. Physical security is to physically protect the network components and entities, e.g. secure rooms for network nodes etc. Information security is to secure the communication or exchange of information in the network. And for this the information content to be transferred should be protected, i.e. we should have secure communication.

To have secured communication we need dedicated technologies which also depend on the type of network being used. There are different security issues in any communication network which are described below.

Confidentiality

Defined by International Organization for Standardization (ISO) as “Ensuring that information is accessible only to those authorize to have access”[9]. From this we can say that only the sender and the receiver can have access to the information being communicated. Confidentiality can be provided by using encryption. If two communicating parties know the secret key, that can be used to encrypt the messages exchanged between them so that the third-party can’t read the message [1].

Integrity

Means the information being exchanged should not be modified other than the sender and receiver, i.e. unauthorized person or entity can’t manipulate the information content and receiver should be able to ensure that the received information has not been manipulated. Integrity can be implemented by using secured Hash or digital signatures [2].

Availability
Availability is the concept through which the authorized subscribers are granted timely and uninterrupted access to the resources of the system [2].

**Authentication**

It is the security aspect in which receiver ascertains the origin of the message. It is used to prove the identity of certain entity [2]. It is the process of establishing confidence in user identities. In authentication process the subscriber provides its identity to the networks and in the response the network grants access to the subscriber [1].

### 2.2 Authentication Process

Authentication is the process in which the identity of the subscriber is verified. To verify the identity, the subscriber provides the additional information corresponding to its identity. After the successful authentication, the access to the network resources and services are provided to the subscriber. The kind of access and services granted depends on the privileges given to the specific entity requesting authentication [31].

Three common types of information are used in authentication of a subscriber to any communication network according to NIST specifications [33].

**Something you know**

It is the subscriber attribute which he knows and normally this can be memorized. Examples include passwords, Personal Identification Number (PIN) etc [33].

**Something you have**

It can be a physical device owned by the subscriber and is usually provided by the network operator on the time of subscription and should be used for authentication. This includes the smart card, token device and so on. Smart card has the capability to process and store the data [33].

**Something you are**

It can be a physical characteristic or part of the body of the subscriber which is stored against his record on the time of subscription to the service. This factor includes the biometric information, retina patterns etc. Every authentication factor has its own benefits and drawbacks; however viability is determined according to the environment in which it is used. Every security level provides more security than the level before it.

**Security in terms of Authentication Level**

In *something you know* the security can be easily breached if the malicious user breaks or guess the correct password. In *something you have*, if the device or the smart card which is used for the purpose of identification and authentication is lost or stolen by someone then the security can be easily
breached. *Something you are* is the most secure level of the above mentioned factors and provides efficient security mechanism as it is based on the credentials that are the body parts of the subscriber and hence it is very difficult for a malicious user to break the security. For strong security solution normally two of these factors are used for authentication [33].

To start the authentication process the subscriber must provide its identity and it can be done by typing the username, swiping the smart card or positioning the face or finger to the scanning device. The identity of the subscriber is verified against some identities stored in the network on the time of subscription. These identities are normally private entities and directly reflect the security level of the system. The process of authentication and identification are correlated and without these the secure access to the system cannot be granted.
The IMS

The fixed and mobile networks have gone through a major transition in the last many years. In the cellular network side 1G systems were introduced in 1980’s and provided basic services for users relating to speech and speech-related services. 1G was evolved to 2G systems in 1990’s through which some data services and supplementary services were offered to the users and in the mid of 1990’s work started on development of 3G systems, which offered faster data rates and various multimedia services to the subscribers [14].

In the fixed network side, the PSTN and ISDN were major networks that provided voice and video communication, as the usage of the internet increased, fast and cheaper connections provided by Asymmetrical Digital Subscriber Line (ADSL) were heavily adopted. By using ADSL subscribers can have always-on connectivity through which they can use real-time communication means.

As with the fast paced development of fixed and mobile networks, the convergence of fixed mobile network is in the progress, and the applications are redefined to provide more services to users. The diversification of ASDL, UMTS and WLAN let to Fixed Mobile Convergence (FMC), and these different access networks can be integrated into IMS, which was standardized by 3GPP [15]. IMS allows applications in IP enabled devices to establish peer-to-peer and peer-to-content sessions easily and securely. Through IMS the multimedia session control in PS domain and bringing CS functionality to PS domain is achieved.

IMS is a global, access independent and standard based IP connectivity and service control architecture that enables various types of multimedia services to the end-users using common internet protocols [14]. IMS services are the multimedia sessions consisting of video, audio and voice, all these media types are mixed in a single session which is supported by IMS. IMS is designed to provide a number of key functionalities required to enable new IP services via mobile networks [15].

IMS delivers multimedia services across fixed and mobile access. It is the only open, standardized way to deliver convenient IP-based consumer and enterprise services to fixed, mobile and cable communities, enabled by one common core and control for all types of networks [16].

IMS provided a platform for delivery of multimedia services which are already available in other IP networks, but with an accurately billing, QoS provisioning, effective troubleshooting and accurate audit of contents download [15].

IMS is designed to bring the value of internet services to both mobile and fixed networks. It helps in the development and offering of advance multimedia applications such as VoIP, Video, Presence and Location based applications and so on [17].
Another issue for the development of IMS is the interoperability of different vendor’s products. Provision of a core infrastructure that support services like session control, security, charging were the driving forces for the developments of IMS. The IMS service platform is designed to assist and control multimedia sessions established between [18]. IMS is an overlay solution that provides interoperability among IP enabled devices using different access networks [19].

3.1 GSM to IMS

The GSM was standardized by European Telecommunication Standard Institute (ETSI) during the 1980’s and after that GPRS network architecture was defined. In 1998 3GPP was founded by organization from different countries and specified 3G system with WCDMA and TD-CDMA radio access, and core network of GSM was evolved. In 2000 release 4 of 3GPP was presented in which originally defined in the draft, All IP core network, was dropped and only some enhancement were made in functionalities like MSC-Media Gateway (MSC-MGW), IP transport CN protocol etc.

The IMS was introduced in 3GPP release 5 and was update in Release 6 & 7. In Release 5 of 3GPP IMS was finally introduced and was supposed to be access independent IP based architecture that can interact with already deployed voice and data networks. Through IMS it was possible to establish peer-to-peer communication with required QoS. In Release 6 of 3GPP the shortcoming of IMS were fixed along with introduction of novel features also the internetworking of the CS, and other IP networks including WLAN were specified. In Release 7 of 3GPP the architecture was enhanced to support fixed broadband connections to the IMS.

3.2 Network Architecture

The vision of IMS was to integrate mobile/fixed voice communication and internet technologies. The two fundamental aspects of IMS to deliver the services it was designed for are IP based real and non real time services and multimedia call model based on SIP. IMS consist of three separate layers that are categorized as connectivity, the session control layer and the application/service layer.

The connectivity layer consists of access and transport layers. As the IMS is access independent and supports all type of access network from wireless to fixed networks and consist of elements at the provider network layer that constitute of IP routers and switches providing IP based transport infrastructure [20].

Control layer consist of services that manage the calls and establishment and modifications of multimedia sessions. Normally these are SIP based
services and the most important are the CSCF. This layer is responsible for all aspects of session states.
The content and application services that provide enhanced service features for IMS enabled networks lies in the service/application layer. At the heart of this layer are the AS and the IP media servers. This is the layer where application logic resides.

3.3 IMS Core Network

The figure 3.1 below depicts the network architecture of IMS, and the main network entities and interfaces especially those involved in the authentication/registration procedure are explained.

3.3.1 Home subscriber Server (HSS)

Home subscriber Server is the master Database for the storage of subscriber’s service related data; the main data stored in the HSS include user identities, registration information, access parameters and service execution [21]. The parameters stored in HSS are public and private user identities, the name of S-CSCF allocated to the user.
The traditional functions of HLR and AuC are also embedded in HSS. So HSS has an important role in the authentication of the subscriber to the IMS [22].

3.3.2 Call Session Control Function (CSCF)

As IMS is SIP based, so the main elements in the IMS network are SIP Proxies or Servers. CSCF provides the end points for the registration and routing for the SIP messages and are backbone of IMS. There are three different kinds of CSCF.

3.3.3 Proxy CSCF (P-CSCF)

P-CSCF is the subscribers first contact point within the IMS. All the requests to or from User Equipment (UE) are forwarded or processed by P-CSCF. P-CSCF is located either in the home network or the visited network [20]. In short the functions performed by P-CSCF are

- Forward the SIP request and response to UE.
- Security Association is maintained by P-CSCF along with integrity and confidentiality protection.
- Handles compressions and decompression of the SIP messages [23].
- Before the subscriber can use the services provided by IMS like multimedia session, the establishment, registration and the signaling messages are forwarded by P-CSCF [20].
3.3.4 Interrogating CSCF (I-CSCF)

It is the contact point within an operator’s network for the connections destined to subscriber of the network and is located at the edge of the administrative IMS domain of an operator. The functions performed by I-CSCF are

- To obtain the address of S-CSCF from HSS.
- Forwarding the SIP requests and responses to selected S-CSCF.
- Performs topology hiding function.

3.3.5 Serving CSCF (S-CSCF)

It is one of the most important and central network elements in IMS and acts as SIP server and SIP registrar. The main function performed are registration and session control. During registration process the S-CSCF performs mapping between the IP address and the public user identity. S-CSCF interacts with the Application Servers (AS) [20].
As the user attempts to register with IMS, authentication data is downloaded from HSS by S-CSCF and sends a challenge to the UE. After the successful authentication, it behaves like a registrar [14].

3.3.6 Application Servers (AS)

Application Servers are the SIP servers where services and applications provided by IMS are executed. They provide service execution environment. AS are used for ease of application development.

3.3.7 IMS terminal

It is an application on the UE that is able to send and receive SIP messages. It can be software on a PC or an IP Phone or a UMTS mobile station. IMS terminal must be equipped with the UICC card containing ISIM.

3.3.7.1 IMS service identity module (ISIM)

ISIM is an application that resides in UICC, which is secure, and temper free device and is inserted into the UE. UICC contains other modules along with ISIM and they can be USIM, SIM etc [25]. The Figure 3-2 shows the content of the ISIM module on UICC. The credentials stored in the ISIM are used to authenticate the subscriber [14]. The data stored in ISIM is categorized as User Identities, Home Network Domain Name, secret key (K), Integrity key (IK) and Ciphering key (CK).

Public User Identity

Is used for registration, and accounting purposes [26] and is stored ISIM module on the UE side and HSS on the network. It is used for routing and through this the subscriber advertises how he can be reached. Telephone number represented in the form of URI like +46762003814@bth.se or an email address like user@bth.se or some other form of SIP URI can be public identities of the subscriber that can be published [25].

Private User Identity

Private user identity is a unique global identity that is used to identify the subscriber [27]. Through private user identity the user’s subscription is defined nor the user. And is used for authentication, accounting and administration proposes. This user identity is represented in the form of Network Access Identifier (NAI) and contained in the entire registration request. The UE cannot modify the private user identity and can be comparable with the IMSI in mobile network.
Derived Identities
If IMS is accessed by the UE which do not contain ISIM module then the public and private identities and home domain name are derived from IMSI. This scheme is used when the UE contains the (U) SIM module.

![Diagram of ISIM and UICC](image)

**Derived Private User Identity**
The private user identity is derived from IMSI in the following way. The username part is replaced with IMSI. The domain name consists of MSS, MNC along with predefined domain name. So if the IMSI is 2341509999999999 where MCC is 234, MNC is 15, MSIN is 09999999999 so the private user identity will be 2341509999999999@234.15.IMSI.3gppnetwork.org [14]. This private identity is neither visible to the end user nor advertised outside of the HN.

**Derived Public User Identity**
In the absence of ISIM module, the public identity is derived from IMSI. This identity is temporary and takes the form of SIP URI. It is derived from the IMSI as follow SIP: user@domain which becomes 2341509999999999@234.15.IMSI.3gppnetwork.org. This temporary public identity cannot be used in any request other than registration and will not be displayed to the end user [14]. Once these identities are used for registration, then the public and private identities saved in the HSS can be learned.

Figure 3-2: IP multimedia Services Identity Module
3.4 SIP in IMS

SIP is a text based application layer protocol developed by IETF for session initiation along with some other functions like notifications and presence, short messaging etc [28]. SIP can establish a new session, modify an existing session or terminate a multimedia session. SIP can also be used to invite a participant to an ongoing session. SIP is used for peer-to-peer communication and uses client-server transaction model. SIP request is generated by client and the server responds to be request by generating a response. The basic request types are INVITE, ACK, REGISTER, BYE, CANCEL and so on. In response to the request there are some basic responses, like 1xx Provisional, 2xx Successful, 3xx Redirect, 4xx Client Failure, 5xx Server failure, 6xx Global Failure.

3.5 Why SIP

The 3GPP has chosen SIP as the protocol for communication of signaling messages between different entities in the IMS network due to its support to almost all type of media and through some modification it can be made more secure and efficient. SIP was chosen to control everything in IMS, due to its vast advantages of being simple, extensible, flexible and familiar [28]. SIP was basically a protocol for communication in internetwork where security and other functions like charging etc are not given more importance. In the internet security was left to end devices where as the telecommunication networks cannot afford security breaches and so they build robust security procedures. For this reason 3GPP had defined many new extensions to SIP with regard to authentication, authorization and charging etc [26]. SIP has been redefined for use within the IMS and so IMS has much better security to the network as compared to conventional VoIP networks.

Some of the examples of extension headers in SIP to be used for IMS are path header for registering, private SIP extension for media authorization, extension header for service route discovery, P-charging vector, P-charging-function-address, P-visited-network-ID etc [14].
4 Authentication Mechanism

There are different authentication schemes employed in different networks. Password based authentication scheme is the most common scheme used, however it is not very secured. It lies in the category of something you know of the security model. This scheme is generally used in internet based authentication mechanism. Subscriber normally chooses the password which is easy to remember and hence is easily cracked by the hackers and can get access to the system. This scheme can be made more efficient if the password used for the access control is intelligently chosen. Many malicious users can use different techniques to obtain these passwords [31].

Authentication using the token falls in the category of ‘something you have’ control solutions. A token is normally a physical device such as an ATM card. ATM card can be used by providing the card itself and the user’s PIN. Tokens can be one time password or the code generator normally used in the banking sector. There are different type of token devices and requires some more information to be used for granting access to the system.

Normally in the authentication schemes employed in this category are challenge-response based schemes, in which the network challenges the subscriber and in the response the user generates a response to the challenge on the basis of which the subscriber is authenticated to the system. This system is more efficient in the form of security as compared to the password based schemes. In challenge-response scheme the subscriber normally sends a random number to the network, known as challenge. The network signs this random number with the secret key, shared by the network and the subscriber, using already agreed algorithm and sends the response back to the subscriber. The subscriber verifies that response is signed by using the shared secret key, and if verified the entities are authenticated [32].

In the following section, the authentication mechanism in GSM/GPRS and UMTS, which are also challenge-response based schemes and employs UICC as authentication token will be discussed and after that a brief overview of the authentication mechanism and schemes used in IMS will be given.

4.1 Authentication in GSM/GPRS

The most important security features in GSM/GPRS system are User Authentication, Encryption of Communication on the radio interface and use of temporary identities. GSM system provides efficient security control by ensuring that the subscriber requesting the service is a valid user. The mechanism used for the authentication of subscriber in GPRS is similar to the mechanism used in GSM.
The goal of authentication in GSM/GPRS network is subscriber authentication, i.e. protection of the network from an unauthorized user. The scheme used for the authentication in GSM/GPRS is based on a simple Challenge-Response protocol. To perform this Challenge – Response mechanism the network and the SIM card utilize the one way hash function [35].

The subscriber authentication in GSM/GPRS is basically the device authentication, in other words the device containing the valid SIM card is authenticated via valid response to the Challenge.

In GSM/GPRS, the Mobile Subscriber is authenticated based on a random number generated in Authentication centre (AuC) and the basis of after the MS request for service by sending its IMSI [10].

4.1.1 GSM/GPRS Subscriber Authentication Mechanism

In GSM/GPRS, the authentication of the subscriber is based on the challenge response mechanism, and the three main entities involved are Mobile Subscriber MS, MSC/VLR or SGSN (in case of GPRS authentication) and HLR. The MS is authenticated to the home network HN via the VLR using IMSI and the master key Ki Stored in the SIM card.

The Master key Ki is stored in the SIM card and the HLR in the HN. When the user connects to the network its unique identity i.e. IMSI stored in the SIM card is sent to the VLR/SGSN of the visiting network which is currently serving the MS. This IMSI received at the VLR/SGSN is sent to the HLR in the HN. The HLR ask the AuC for triplet containing the RAND, Signed response SRES, and a session key Kc for encryption. The AuC calculates the Random number RAND by using random number generator, the SRES by using the one-way hash function A3, and the Kc by using the other function A8 [10].

The SRES is calculated by the function A3 in which the RAND and Ki are used as input, also using these same two values as an input to another one way hash function A8, the encryption key Kc is generated.

The SRES computed at AuC is sent to the VLR via HLR along with the RAND and Kc. The VLR saves the SRES, Kc and forwards the RAND as a challenge to the MS. In the MS at the SIM card RAND is used again by the same function A3 along with the secret key Ki to generate the response RES. The RES value calculated in the MS is sent to the VLR which compares it with the SRES which was already saved. If the SRES is same as RES received then the subscriber is authenticated.

The triplet (RAND, SRES, Kc) generated at the AuC should not be calculated every time when the authentication request is received, but the AuC can calculate a set of triplets in advance and save them in HLR and at least five triplets are sent to the VLR on demand. The VLR uses triplet only once for authenticating the user, for subsequent authentication request new triplet from the stored triplets in VLR is used.
In this process of challenge response authentication the RAND sent from the VLR to the MS is the challenge and the RES calculated at the MS and transmitted to the VLR is considered as a response to the challenge.

4.2 Security Mechanism in UMTS

The security architecture of UMTS is based on the security mechanism of GSM. Most of the functions and concepts are borrowed from GSM, however certain changes were made to overcome the weak security of GSM and hence new functions are added to enhance the security. Some of the major enhancements to the security in UMTS are

- Mutual authentication
  The user can identify the network and network identifies the user.
- Explicit Integrity
  Data integrity is assured explicitly by use of integrity algorithms.
- Network Security
  Mechanisms to support security between networks nodes.
- Switch Based Security
  Security is based within the switch rather than the base station.
- IMEI Integrity
  Integrity mechanisms for IMEI provided from the start.

The access security is classified into authentication, confidentiality and data integrity. The main focus of this part will be the Authentication. UMTS authentication provides mutual authentication [39], meaning that the network authenticates the subscriber and also the subscriber makes sure that it is communicating with the legitimate network. Details about the exact mutual authentication procedure will be discussed in the next section.

4.2.1 UMTS Authentication

UMTS authentication provides mutual authentication, the UE initiates the Authentication procedure by sending the authentication request in the form of either the IMSI or the Temporary IMSI (T-IMSI) or the Packet IMSI (P-IMSI) used for PS domain of the CN.

The entities involved in the authentication procedure are
- Home Network HN
- Serving Network SN
- Terminal (UE with UICC containing USIM).

The authentication procedure in UMTS is carried out by Authentication and Key Agreement (AKA) protocol.
4.2.2 AKA Prerequisites

The USIM and the AuC share the 128 bit master key and the authentication functions. AuC has the random number generator and also fresh sequence numbers SQN are generated by the AuC, whereas USIM has the scheme to check the freshness of the SQN.

4.2.3 UMTS AKA

UMTS AKA is a security mechanism based on a challenge/response authentication protocol. A challenge/response protocol is a security measure intended for an entity to verify the identity of another entity without revealing a secret password shared by the two entities [39].

The Authentication process starts with the initiation of authentication request by the UE by sending the IMSI or (T-IMSI/P-IMSI). The process is shown in the Figure 4-1. This request is sent to the VLR/SGSN in the serving network SN which further sends it to the HN. The AuC in the HLR of HN processes the authentication request. The shared secret key K is stored in the HLR against the IMSI of the subscriber and based on this, authentication vector is computed. The AuC uses IMSI to generate a random number RAND (128 bits) and a SQN 48 bits. This SQN is chosen in ascending order in order to later check the freshness of the SQN. These RAND, SQN and secret key K are used as an input to the functions f1-f5 to generate the authentication vector AV [35].

The authentication vector consists of the following parameters: the Expected Response (XRES) generated using the f2 function and is 32 – 128 bits; the Cipher Key (CK) generated using the f3 function and is 128 bits; the Integrity Key (IK) generated using the f4 function and is 128 bits; the Authentication Token (AUTN), which is a concatenation of different parameters and is 128 bits.

This authentication vector AVs generated at the AuC is transferred to the VLR/SGSN in the SN. The SN selects one AV and challenges the UE by sending RAND and AUTH fields from the AV [10].

This challenge is used in the USIM along with K as inputs for the authentication procedure on the USIM side [39].

The USIM using the secret key K verifies that the received challenge data could only have been constructed by someone who had access to the same secret key K. The USIM will also verify that the AV has not expired by checking its sequence number (SNQ) field.

The output generated at the USIM consist of the following keys; Response (RES) 32 – 128 bits, generated by the f2 function, the SQN 48 bits, the Cipher Key (CK) and the Integrity Key (IK), generated by the f3 and f4 functions respectively.

The terminal sends the computed response RES to the serving network which compares it with the XRES stored in the SN extracted from the Authentication vector generated in the HN. If both the XRES and RES match then the user is authenticated.
The USIM and the VLR/SGSN have authenticated each other after two conditions have met: First, that the USIM has verified that the MAC field in AUTN equals a value computed internally using the key K and the fields SQN, RAND and AMF. Second, the VLR/SGSN has verified that the RES value transmitted by user’s mobile station equals the internal XRES value.

4.3 Authentication in IMS

The IMS was introduced by 3GPP and also adopted by TISPAN for fixed-mobile communication. IMS is overlay architecture and require strong security solution to be implemented to protect data transmission, confidentiality, authentication, integrity and anti-replay. The potential security threats to IMS are denial-of-service attacks, misuse of application and services, attack on SIP signaling and threats to IMS access link. 3GPP specifies the security mechanism in IMS in the form of security levels, and these are the authentication and authorization of the user, and to protect the network resources and the confidential information of the user. Based on the specifications the security in IMS can be classified into Access domain security and network domain security. Access security is to protect the unauthorized access to IMS domain and it is independent of its underlying access network security features. Access security i.e. authentication of the subscriber is based on the UMTS AKA mechanism.
in which mutual authentication between the subscriber and the network is carried out [14]. IMS access security is based on IETF, 3GPP and TISPAN specifications and standards and called IMS AKA in which along with the authentication of the subscriber and the network the confidentiality and integrity keys are generated which are further used to protect the communication on the link. The key thing to accomplish the access security is to the authentication of the subscriber and the protection of the SIP signaling between the UE and P-CSCF.

4.3.1 Security Architecture

Network domain security (NDS) in IMS is to protect the links between the network elements within the IMS network. In NDS the integrity, authenticity and confidentiality of SIP signaling and IP media traffic is ensured by using cryptography, node hardening and virus protection etc. Protection in network domain is carried out using the IPsec/IKE [36]

The Figure 4-2 shows the security architecture of IMS in which five different security associations (SA) are depicted.

Figure 4-2: IMS security architecture

- SA 1 provides the mutual authentication between the UE and S-CSCF. The shared secret key (K) stored in UICC and AuC in HSS is used for authenticating the private user identity and registering the public user identity.
- SA2 provides a secure link between UE and P-CSCF for protection of communication on the Gm interface, on which the user’s signaling messages are transferred to and from P-CSCF.
- SA3 provides security for the communication between the I/S-CSCFs and HSS. It is used for network domain security in which the messages exchanged on Cx interface are secured.
• SA4 provides secure communication between the different SIP CSCFs when the P-CSCF is in the visited network.
• SA5 provides secure communication between the different SIP CSCFs when the P-CSCF is in the Home network [36].

4.3.2 Authentication Schemes in IMS

Different authentication schemes can be applied to IMS, other than specified in the IMS related specification of 3GPP and TISPAN, because of different types of access networks and access devices. As IMS can be accessed from different networks like cellular network, ADSL network, Wi-Fi network, Fixed line network etc. So, if the user switches to another device let suppose from cellular network to a fixed line phone then the authentication token that can be SIM in cellular network is no longer usable in fixed line network, so the authentication schemes would be certainly changed in the other network [34]. So the authentication schemes

![Diagram of Access and Network Domain Security](image)

Figure 4-3: Access and Network Domain Security
that can be used with different type of access devices or the access networks can be different. However as shown in the figure below, no matter what ever type of access network is, the IMS authentication is performed between the IMS client and the P-CSCF in the IMS network. It doesn’t depend on the type of the access network. The figure shows the different security mechanism in the IMS network, the link between the ME and RNC is secured by the Access network security, here the access network can be any IP based network, which can provide IP connectivity to the Subscriber to access the services provided by IMS. Then there is shown the IMS access level security i.e. authentication of the IMS client to the IMS network, and lastly the Zb interface shows the network domain security between different IMS entities within the network.

For the Mobile phone the authentication schemes will be based on SIM/USIM/ISIM. The authentication schemes that can be used with Laptop or PC can be username/password scheme, private/public keys, one time password, MAC-address etc. The authentication schemes when PDA is used to access IMS services can be username/password or one time password.

4.3.2.1 UICC Based Authentication Schemes

The scope of this thesis work is to study and evaluate the authentication schemes that can be used to access IMS services when the access network is of any type, but the user device has the support to the UICC which can be utilized as a token for authentication.

So we can say that for the authentication levels defined by National Institute of Standards and Technology, in the form of “something you have”, “something you know” and “something you are” the UICC based authentication schemes achieve the first two levels in the form of UICC as something you have, and a PIN to activate the UICC as something you know [34].

The UICC based authentication Schemes in IMS can be further classified as ISIM/USIM based and early IMS security using GSM/GPRS access network. In ISIM/USIM based authentication scheme the implementation depends on the number of factors which can be that, is the given IMS network fully compliant IMS network and the other is that whether the UE is capable of supporting the ISIM/USIM [8]. In the second scenario it can be that the given IMS network is an early implementation of IMS network which do not at the moment support the ISIM or the UE is not capable of supporting the ISIM. In this case interim IMS authentication mechanism is used.

In the next chapter a detailed overview of the authentication schemes using ISIM/USIM and the early IMS authentication mechanism will be given.

ISIM/USIM based IMS authentication mechanism utilizes UMTS Authentication and Key Agreement (AKA) protocol for mutual authentication of the subscriber and the network by utilizing the shared
secret key (K) and produces integrity and confidentiality key for further securing the communication.

The Early IMS authentication mechanism relies on the access security of underlying access network and creates a secure binding in the HSS between the public / private identity and the IP address currently allocated to subscriber at the bearer level [38]. And the access network in this case is GPRS network or PS domain of the UMTS network.
5 IMS Authentication Schemes

Secure access to IMS deals with the protection of the signaling between the Subscriber and IMS and the mutual authentication, i.e., authentication of the subscriber by the network and the network authentication by the subscriber. Mutual authentication in IMS is performed by SIP Register request sent from the subscriber to the home network. In response to the register request, the home network will send a challenge to the subscriber.

At the UE side, the module used for mutual authentication is ISIM which contains the SIP identities, i.e., IMS Private user Identity (IMPI) to be authenticated and IMS Public user Identity (IMPU) to be registered. ISIM also contains the keys and functions used in the authentication process [11].

Mutual authentication between the subscriber and the network is carried out by the subscriber sending the Register request to the HSS in the home network, along with its identities [15]. The HSS generates and sends the challenge to the UE through S-CSCF. The UE computes the response to the challenge and sends it to the serving network, which is compared with the one sent by HSS. If both of these match then the subscriber is authenticated. Also, before sending the response to the challenge, the UE authenticates the network by comparing an attribute in the challenge with the one generated at the UE. If those two also match then the network is authenticated by the UE [14]. The figure 5-1 shows the secure access architecture to IMS. In the figure it is shown that the AKA is run between the UE and the HN, whereas the IPsec SA is established between the UE and P-CSCF which normally lies in the visiting network.
5.1 Authentication using IMS AKA

In this section, the IMS AKA procedure for the authentication is discussed. For IMS AKA to work, the subscriber should have an ISIM module on the UICC inserted in the terminal equipment. ISIM module contains along with the SIP identities the shared secret key (K) to be used for authentication [14]. To get access to IMS, the subscriber sends a Register request to the IMS entry point P-CSCF. The P-CSCF will forward the request to I-CSCF which will select the S-CSCF serving the user and forwards the request to it. The S-CSCF after getting the request containing the IMPI and IPMU, request the Authentication Vector (AV) from the HSS. The AV request contains the IMPI and the number of authentication vectors desired. The HSS responds with an ordered array of ‘n’ authentication vectors to the S-CSCF. Each AV can be used for one authentication request. AV contains random number RAND, authentication token AUTN, expected response XRES, confidentiality key CK and Integrity key IK [10].

S-CSCF extracts and saves the XRES and sends the remaining authentication challenge to the P-CSCF via I-CSCF. P-CSCF stores the CK and IK and forwards the challenge containing AUTN, IMPI and RAND to the UE. UE takes the AUTN parameter from the challenge and discovers MAC and SQN by using different functions. The UE verifies that the SQN is in correct range and calculates the XMAC. If the MAC extracted from the AUTN received in the challenge matches the XMAC calculated at the UE, then the UE verifies the authenticity of the network, and calculates the response RES to the challenge. This RES is sent to the S-CSCF via second register request and is compared with the XRES stored at S-CSCF. If both the RES and XRES match then the subscriber is authenticated, and the IMPU is registered.

By this procedure the network and the subscriber have authenticated each other. Also, the CK and IK generated along the AV in HSS and stored at P-CSCF, works in collaboration with the CK and IK calculated in the UE to secure the communication between the UE and P-CSCF by establishing the IPsec Security Association (SA) [43].

5.2 ISIM Based Authentication

Before a subscriber can use the services provided by IMS, he/she must have an active registration to the IMS network, and to get registered with the network the subscriber sends a SIP Register request to the IMS network. The authentication of the subscriber is carried out in the process of registration. The UE’s register request is sent to the P-CSCF, which is the subscriber’s first point of contact to the IMS network. The address of the P-CSCF is discovered by the UE in the process of GPRS attach procedure, through DHCP or method depending on the type of underlying access network providing IP connectivity.
The UE sends the Register request to the P-CSCF. This request is constructed by the UE which we suppose that is in the visited network and uses Digest AKA in the SIP register request for the authentication procedure. The UE construct the Register request by using the following headers in the request i.e. Request-URI, Via, Max-Forward, P-Access-Network-Info, From, To, Contact, Authorization, Security-Client and Supported. This request is forwarded to the P-CSCF [23].

The P-CSCF when receives the request, discovers from the URI that the UE is registering from the visited network and hence finds the address of the I-CSCF by sending a DNS query to the server [23]. After finding the address of the I-CSCF the request is forwarded to it by P-CSCF. The integrity protection flag is set to ‘no’ showing that the subscriber has not been authenticated [14].

The I-CSCF when receives the Register request from the P-CSCF, sends a Cx query i.e. registration status query based on diameter protocol by sending the IPMU, IMPI and visited network identifier to HSS to identify the subscribers registration status [15]. Based on the response to the query, the I-CSCF selects the S-CSCF, and forwards the Register request containing along with other headers the authorization header by adding its entry in the Via header [23].

The S-CSCF when gets the Register request, came to know that the request is not integrity protected and hence the subscriber should be challenged. The Subscriber is challenged by sending an AV which consist of random number RAND, an expected response XRES, integrity key IK, confidentiality key CK and an authentication token AUTN [43].

```
Figure 5-2: AV generation at network
```

The S-CSCF now challenges the UE by sending a SIP 401 Auth-challenge to the UE via I-CSCF by picking the one AV, excluding the corresponding XRES; this XRES along with the RAND is stored in the S-CSCF[10]. P-CSCF receives the 401 authn-challenge, stores the CK and IK from the WWW-Authenticate header, and sends the remaining message to the UE. These keys CK and IK are used for establishment of Security Association (SA) between the UE and P-CSCF.
UE when receiving the 401 authn-challenge, extracts the MAC and SQN from the AUTN parameter, and compares it with the XMAC calculated at the UE by using RAND, if both the MAC received and the XMAC calculated are equal and the SQN is in correct order, the network is authenticated by the UE. After performing these tests the UE calculates the RES to the challenge and computes the keys CK and IK. The response RES is sent to the S-CSCF in the authorization header of second register request via P-CSCF and I-CSCF [23].

![Figure 5-3: AV generation at ISIM](image)

The PCSCF on receiving the second register request containing the authorization challenge response checks that the request was not altered on its way from UE to it [15]. Then the P-CSCF again finds the I-CSCF through the DNS procedure stated earlier. And through the I-CSCF the request is forwarded to the S-CSCF [14]. SCSCF when receives the Register request, extracts the RES and compares it with the, XRES was already stored in the S-CSCF, if both are equal then the UE with the IMPI is authenticated and the IMPU is registered [23]. After successfully authenticating and registering, the S-CSCF informs the HSS in Server-Assignment-Request (SAR) based on diameter that the subscriber has been successfully registered. In response, the HSS will download through the Server-Assignment-Answer (SAA) the user profile into the S-CSCF [43]. In the last the SCSCF sends the 200 OK message to the UE through I-CSCF and P-CSCF that the user has been registered.
Figure 5-4: IMS AKA Registration/Authentication signaling flow

5.2.1 USIM Based Authentication

The identity used for authentication in IMS is IMPI, stored along IMPU on ISIM application on UICC. However as with the deployment of IMS there will be lot of terminals which don’t support ISIM or the operator is not in the position to upgrade all of its customers UICC containing ISIM, but the users of such terminals have the subscription of IMS. So for the subscribers who have IMS subscription but don’t have ISIM supported terminal can use the USIM application on there UICC card to have a secure access to the IMS. The USIM application is described in cellular networks chapter. The USIM does not contain the Private and Public User Identities but USIM along with the other data contains the IMSI which is used by the IMS terminal to derive the identities IMPI and IMPU used for IMS access [25].

The authentication mechanism to IMS using USIM is same as ISIM with slight differences. The IMPI used as user name in authorization header and the request URI containing IMPU are derived from the IMSI stored on the USIM application. The derivation of these identities from ISIM has been explained in 3.3.7.1. As these identities are derived from IMSI which is
never exposed to the outside world and is securely stored on the temper free smart card so these derived identities should not be used other than initial registration request.

As the subscriber with USIM on his terminal issues a request to access IMS, the IMSI is extracted and IMPI and IMPU along with Home network domain name is derived. Then the registration request containing these derived identities in the SIP Register request are sent to S-CSCF in the same way as was done when ISIM was in use. The HSS and the USIM use the stored long term secret key K for the authentication and registration.

On the successful mutual authentication of the network and the subscriber, the IMPU is registered [25]. The home network will not disclose the IMSI derived IMPI and IMPU outside of the network The S-CSCF sends 200 OK response to the UE in which it also sends P-Associated-URI header which contains list of all the IPMUs associated with the user. The first IMPU in the list of P-Associated-URI is normally a registered IMPU, which the subscriber can use for further request and responses [14]. From now onward the subscriber can’t use the IMSI derived IMPU in any of the SIP messages. The session establishment from the IMS terminal with the derived IPMU will be rejected by the S-CSCF.

5.3 Early IMS Security

IMS is designed to provide a number of key functionalities required to enable new IP services via mobile networks. Services that are provided by the IMS include push-to-talk, instant messaging, presence and conferencing etc. As, these services will be provided by the IMS architecture specified by 3GPP in its specifications, there will be some situations in which early deployment of IMS will be required, which will be an interim solution and gradually moved to the full functional IMS. These early deployment may lack some of the services and architectural requirements of the original design, and this can be due to different reasons. These Pre-IMS deployment will be only due to lack of support of ISIM module on the terminal or for the quick implementation of the IMS. But these deployments will be mostly due to the UE and the access network used by the subscribers for accessing the IMS, so it should not create any design or architectural change in the IMS Core network. One of the main reason for the early IMS is the lack of support of the IMS enabled UICC card by the UE. This is due to the fact that when there will be an implementation of IMS a lot of subscribers will be having the mobile terminals which will not support the ISIM module i.e. 2G only devices and on the other hand it will be difficult for the network operator to upgrade all the subscriber base with the new UICC card that will be supporting the IMS. The main problem is the support of IMS identities used to access and receive services from IMS by the SIM card used by the GSM subscribers. Also, the lack of support of IPsec by most of the UE is a reason for deployment of the Early IMS solutions [38].

37
The other reason can be the non-compliance of IPv6 by the UE and the network equipment, as specified by the 3GPP the IPv6 will be exclusively used for IMS. So, for an interim solution there should be an architectural design that can be introduced to support these problems, which will be later on moved to fully compliant solution. So for these reasons Early IMS solutions were introduced [23].

Although the security features which provide the most efficient and reliable security mechanism are preferred but in the early IMS implementation the fully compliant security solution will not be supported. And to overcome the security threats to the IMS network an interim security solution was proposed to protect against most significant security threats. This solution was given the name Early IMS access security, as the interim solution was introduced just due to the lack of support on access level. This solution implements absolutely no IMS security but relies on the authentication of the subscriber on the underlying access network and the IP addresses are sent to IMS network as a proof of authentication [40]. The interim solutions work when the UE is having the SIM or USIM module on the UICC. It is recognized that the early IMS security solution is simpler than the fully compliant IMS security solution; it should provide significant protection against most common security threats. As the early IMS security solution was introduced to support early IMS deployment it should be considered as an interim solution and be upgraded to the IMS security as proposed in the specifications. Early IMS security solution can coexist with the full functional security solution deployment so the SIP/IP core should be able to differentiate between the early IMS security and fully compliant IMS security subscriptions. The interim security solution is provided only for the access networks of type GPRS or PS domain of UMTS network, and in this sense it doesn’t provide a high degree of access independence [23].

The authentication mechanism in early IMS security works by secure binding between the SIP identities and the IP address assigned to the subscriber by the access GPRS or the PS domain of the UMTS network. In other words, the early IMS security uses the GPRS or UMTS PS CN authentication as it verifies that the IP address in the IMS access request issued by the subscriber is same as the IP address allocated to it at bearer level [38]. Subscriber authentication to IMS by using SIP register request is linked to a Packet Data Protocol (PDP) context. For PDP context establishment IMSI is used whereas for authentication/registration to IMS IMPI are used, so there is one-to-one relationship between IMSI and IMPI. SIP identities used for access to IMS will be derived from the IMSI as explained earlier. However, these identities cannot be used other than register request so the implicit registration is mandatory to register the subscribers IMPU(s) [14].

In early IMS security a dependency between the SIP and IP bearer is created by binding the IMS transactions to the GPRS or UMTS PS domain security. Hence the interim solution doesn’t provide a high level of
security as compared to fully compliant security solution, where a separate security association is established between the UE and the IMS network. In the interim solution it is required that the HSS should be equipped with the subscription data before a SIP Register request is accepted [38].

5.3.1 Authentication Procedure

For a subscriber to access the services provided by the IMS, it should have a registration with the network and for this the subscriber uses SIP register request. The SIP register request is sent from the UE to the SIP server in the IMS network which authenticates and registers the subscriber after which, the services are available to use. The SIP registration procedure in case of early IMS security is depicted in the Figure 5-5 and is described in this section [38].

Before a mobile subscriber can start an IP session over GPRS network, it must perform the registration procedure, which is formally referred to as GPRS attach. In GPRS attach procedure subscriber informs that it wants to have an access to the GPRS network. And after the successful attach procedure user is permitted to access the network in secure fashion. However to access an external network like IMS or any other Packet Data Network (PDN) it must have an active Packet Data Protocol (PDP) context established.

To establish a PDP context the UE sends an activate-PDP-context request to the SGSN, which select the GGSN [7]. Then the SGSN sends the create PDP context request to the GGSN which assigns a PDP address i.e. an IP address to the received request after certain confirmations and then sends Accounting Request start to the HSS which includes the allocated IP address, the IMSI and MSISIDN. The HSS stores the IP address against the derived IMPI from the IMSI. The IMPI is derived from the IMSI following the procedure explained in the 3.3.7.1 [41]. HSS after saving the IP address against the IMPI sends a response to the Accounting-request-start-answer to the GGSN. On receiving this GGSN sends a create-PDP-context-response to the SGSN, which further sends the activate-PDP-context-accept to the UE along with the IP address allocated to the PDP context and the address of the P-CSCF.

After the UE gets an active PDP context it sends a SIP register request to the SGSN which forwards the request to the P-CSCF. The register request is created by the UE in which the From header contains the IMPU derived from the IMSI, along with the other headers, but the authorization header which contains the IMPI and security-client header are not included in this request [38].

The P-CSCF when receives the Register request, will check the IP address in the sent by parameter of the ‘‘via’’ header which should contain the source IP address from which the packet was received. On receiving the register request that doesn’t contain the authorization header and the security client header, the P-CSCF will include an entry in the Path-header identifying itself and forward the request to the I-CSCF [14].

39
The I-CSCF when receives the Register request from the P-CSCF, sends a Cx query i.e. registration status query by sending the derived IPMU, IMSI and IP address to HSS to identify the subscribers registration status. Based on the response to the query, the I-CSCF selects the S-CSCF, and forwards the Register request not containing the authorization header to it [23].

The S-CSCF when receives a Register request without an authorization header, identifies the derived public user identity from the To header and IP address from the Contact header. The S-CSCF will send a Cx MAR command to HSS which contains the Derived IMPU from the To header and IP address from the Contact header [38] [23]. For this the HSS extracts the IMSI from the derived IMPU and retrieves the IP address stored against the IMSI at the time of PDP context establishment. The HSS sends this IP address associated with the IMSI to the S-CSCF in the MAA command [42]. The S-CSCF then compares this received IP address from the HSS with the IP address received in the Contact header of Register Request. If both of the IP addresses match i.e. that the address saved in the HSS is same as the address received in the Register request the subscriber is authenticated by the S-CSCF. As the subscriber is authenticated the S-CSCF sends a SAR to update its name in the HSS against the registration and downloads the data related to the user’s profile. After this the S-CSCF sends a 200 Ok response to the UE via I-CSCF and P-CSCF along with the P-Associated-URI header [14]. The P-Associated-URI header contains the list of SIP URIs and tel URIs which are associated with the subscriber. In this list at least the first URI i.e. IMPU is registered and can be used for further communication by the subscriber [38].
Figure 5-5: Early IMS Registration/Authentication signaling flow
5.4 One Pass GPRS-IMS Authentication

This section is an excerpt from the article taken from IEEE journal for communications, One-pass GPRS and IMS authentication procedure for UMTS, by Chang, Meng, Lin and Bing. The one pass GPRS-IMS authentication method was proposed in IEEE journal for efficient authentication of UMTS subscriber to IMS. For the subscriber to use UMTS PS-CN the 3GPP AKA is performed and IMS AKA is used for the authentication of IMS client to access and use the services provided by IMS. As IMS AKA is based on UMTS AKA so the subscriber has to go through two pass authentication mechanism of 3GPP AKA and IMS AKA, in which most of the steps and procedures are repeated. So to overcome this issue the one pass method was proposed to increase the efficiency of the subscriber authentication. In one pass method the Subscriber first gets authenticated to the UMTS PS-CN, which is evolved from GPRS network and the identity used for the authentication is IMSI. As the IMSI has been correctly authenticated then the proposed solution specifies that instead of repeating the same steps for authenticating the IMPI for IMS network access, the (IMSI, and IMPI) pair should be used for the IMS client authentication. In this method the IMPI is authenticated on the basis of the authenticated IMSI of the access network, however the explicit IMS authentication is not performed.

Using this method the IMS client is authenticated to the network by efficiently avoiding the 50% of the network registration/authentication traffic and the storage from buffering the AVs.

The one pass GPRS-IMS authentication as shown in the Figure 5-6 can be explained as follows. However the solution assumes that the SGSN is configured with the SIP application Level gateway (ALG).

The MS after getting authenticated to the UMTS PS-CN and PDP context establishment sends a SIP Register request to the SGSN with the parameter IMPI to be used for authentication. The SGSN identifies the IMSI from the GPRS packet received for the MS and the SIP ALG adds this IMSI to the IMPI in the register request and forwards the request to the P-CSCF. The P-CSCF forwards the request to the I-CSCF which finds the S-CSCF for the subscriber via UAR/UAA message exchange between the I-CSCF and the HSS. The Register request containing the IMSI and IMPI pair is sent to the S-CSCF. This (IMSI, IMPI) pair is stored in the S-CSCF and SAR is sent to the HSS using the IMPI. On the basis of received IMPI the HSS finds the IMSI value already stored at the time of subscription in the database and this IMSI value is denoted as IMSI_{HSS} (impi). The name of the S-CSCF serving the subscriber is stored in the HSS and SAA request is sent to the S-CSCF by the HSS with the retrieved IMSI against the IMPI and the user profile. The S-CSCF compares the
stored there from the register request sent by the I-CSCF with the IMSI value retrieved from the HSS, if both values match each other then the subscriber is authenticated and the 200 OK message is sent to the UE by the S-CSCF via I-CSCF, P-CSCF and SGSN.
This method correctly authenticates the subscriber to the ISM network based on the GPRS authentication and in the process no IMS level authentication is performed. In other words we can say that in one pass GPRS-IMS authentication mechanism, the IMS level authentication is performed by linking to the access network authentication.

5.5 Evolutionary IMS AKA

This section is an excerpt from the article taken from the Computer journal, Efficient and Provably Secure IP Multimedia Subsystem Authentication for UMTS by Chung, Jian. Evolutionary IMS AKA (E-IMS AKA) was proposed as research work published in the Oxford Journal. The E-IMS AKA is used as a short form for the title of the article Efficient and provably secure IMS authentication for UMTS. The solution was proposed for IMS in UMTS framework but can be applied to the next releases of the 3GPP IMS architecture in which IMS was defined to be access independent and can be accessed from almost every type of communication network. So E-IMS AKA can be applied to every UE regardless of the access network but the condition is that the UE must support the UICC containing the USIM/ISIM module. E-IMS AKA
provides efficient and reliable subscriber authentication using the UICC. In this authentication method the security architecture of IMS AKA is maintained however the efficiency is increased by avoiding the duplicating IMS registration messages. After the access network authentication the UE sends a register request to the IMS network which contains the RAND, IMPI, and the digest response calculated at the UE. The request is forwarded to S-CSCF which calculates its own digest response based on the algorithm used on the UE side. If both the digest responses are equal the UE is authenticated. The S-CSCF exchanges the SAR/SAA message with the HSS to register the UE and to calculate the authentication response, which is sent to the UE in 200 OK message. The UE calculates the authentication response and if it match with the one received from the S-CSCF, the network is authenticated.

5.5.1 Detailed Procedure

E-IMS AKA (depicted in the Figure 5-7) can be decomposed into the following steps:
Before sending the SIP register request the UE performs following steps:
The RAND\textsuperscript{j} is computed using the time stamp (TS), which is selected from the universal time and RSN, is calculated by using the equation (a) given below.

$$RSN_j = RSN_{j-1} + INC$$ \hspace{1cm} (5-1)

Here in the equation RSN is the random value and lies between the range \{1.....32\}. So the

$$RAND_j = TS_j \| RSN_j$$ \hspace{1cm} (5-2)

For the initial Registration the UE must have the IMS temporary key (ITK) which is calculated by

$$TIK = CK \| IK$$ \hspace{1cm} (5-3)

Here the key CK and IK are calculated by using the RAND\textsuperscript{j} and shared secret key K stored on ISIM module as an input to the one-way hash functions. The digest password (DP\textsubscript{u}) is computed by using the MD5 algorithm and in which string1 is used which is he http-digest-aka password.

$$DP_u = PRF(RAND_j \| ITK, string1)$$ \hspace{1cm} (5-4)

Here in this method the subscript \(j\) denotes that whether the registration request is initial registration or the subsequent registration. When \(j=1\) it shows initial registration and when \(j >1\) it means that the request is for subsequent registration is raised.
Now the UE sends a SIP Register request to the S-CSCF via P-CSCF and I-CSCF containing the IMPI, RAND, and the digest-response, which is computed from the DP. S-CSCF confirms the whether the TS is between the acceptance window size and stores the RSN. IMPI along with RAND is sent to HSS in MAR command on Cx interface. The HSS computes the CK and IK from the one-way hash functions with input value RAND and K. These keys are sent to the S-CSCF along with the subscriber profile in Cx MAA message.

S-CSCF derives the ITK by using the received keys CK and IK employing eq. (5-3). This ITK should be equal to the ITK derived at the UE. The S-CSCF computes the digest response by using the $DP_{uj}$ calculated using eq. (5-4). This digest-response is compared with the one received in the Register request, if both match then the UE is authenticated and the SAR/SAA messages are exchanged between S-CSCF and HSS to register the UE.

Now the S-CSCF performs the following computation

$$DP_{uj} = PRF(RAND_{j} + 1 || ITK, \text{string1})$$ (5-5)

$$IPsec-CK_{j} = PRF(DP_{uj} || DP_{s} || ITK, \text{string2})$$ (5-6)

$$IPsec-IK_{j} = PRF(DP_{uj} || DP_{s} || ITK, \text{string3})$$ (5-7)
In these equations above, the string2 and string 3 parameters are the http-digest-aka of cipher key and integrity key respectively. Now the authentication-response to be used in Authentication-info header is calculated using $DP_{sj}$. And the SIP 200 OK message is sent to the UE containing the CK and IK along with the authentication-response via I-CSCF and P-CSCF. The P-CSCF extracts and saves CK and IK for establishment of security association (SA) before forwarding the message to the UE.

The UE uses the equation (e) to compute $DP_{sj}$ where RAND and ITK are used which were calculated by the UE. If the authentication response calculated from $DP_{sj}$ is equal to the authentication response received in the 200 OK message then the network is authenticated by the UE and in this way the mutual authentication is achieved between the UE and the IMS network. The CK and IK are used to form SA to protect the communication between the UE and P-CSCF.

This proposed method efficiently and correctly performs the mutual authentication between the UE and the network along with the establishment of SA, however using this scheme a lot of unnecessary signaling traffic used for authentication/registration in IMS AKA challenge response architecture can be avoided.
6 EVALUATION

We deal in number of ways to make authentication procedure more vital, otherwise it severely effects information, data protection/integrity, service and network resources costs, reliability, efficiency and many fraudulent problems. We focus on UICC based IMS authentication schemes and they can be categorized based on the type of module implemented on the UICC in the user equipment i.e. SIM/USIM/ISIM. We proceed in evaluating these schemes in terms of the three parameters which are security, user friendliness and complexity.

6.1 Evaluation Based on Security

The security aspect of authentication schemes will be categorized into three aspects to carry on the evaluation.

6.1.1 Authentication Level

The NIST electronic authentication guideline (described in 2.2) define three authentication levels i.e. “something you have”, “something you know” and “something you are”. In an ideal situation all the three together provide the highest level of security, but realistically if any schemes implement only two of these factors i.e. “something you have” and “something you know”, it is assumed to be the acceptable security level.

All the UICC based authentication schemes under observation employs two level authentication. In the first level, subscriber holds physical token in the form of UICC which is regarded as “something you have”. For the UICC activation, the subscriber must know the PIN code, which is regarded as “something you know”. However this PIN can be disabled either by the subscriber or the service provider. So the authentication schemes based on UICC fully provide two factor based security at higher satisfaction.

In order to access the network, UICC along with valid PIN is required. If the UICC is lost or stolen, it can pose a real security risk but if the second factor is also implemented, then the person who got the lost or stolen UICC can’t access the network if he doesn’t knows the PIN. So the malicious user must know the PIN if he is in possession of the UICC to get access to the network.

All the UICC based authentication schemes shows that the level of authentication is same as every scheme uses UICC and PIN mechanism, which are regarded as something you have and something you know respectively.
6.1.2 Timeout and Re-Authentication

For every kind of security implementation in the communication networks, re-registration is important to ensure security level. Timeout and re-authentication mechanism specifies the timestamp for which UE will remain authenticated with the network until the timeout occurs. Re-authentication mechanism provides greater level of security but can decrease system performance, increases delay and complexity.

For IMS subscriber’s authentication SIP Register request is used which perform authentication along with the registration. In SIP Register request there is a registration timeout mechanism, which specifies the time until the current registration will be valid. This timeout mechanism is implemented by “expire” parameter in the Contact header of SIP Register request. After timeout expiry UE have to request re-registration/re-authentication in order to keep the session active.

All UICC based registration/authentications schemes under observation uses SIP register request by default so they contain “expire” parameter required for timeout and re-authentication mechanism, through which the subscriber has to re-register itself to have more security. And hence we can conclude that all the schemes (discussed in 5) exhibit similar qualities in terms of timeout and re-authentication process. As the re-registration mechanism is used in the SIP register request used for registration, and greatly enhances the security by periodically re-registering the user.

6.1.3 Security Attacks

Communication network is an open door for all kind of security breaches but proper security mechanism safeguards such threats and violations. Most of the security attacks are related to authentication and hence used for unauthorized access to resources and information. So an authentication mechanism implemented in the network should be strong enough to prevent some of the common attacks related to authentication.

There are a number of common security attacks i.e. man in the middle (M-i-t-M), eavesdropping, reply attacks, session hi-jacking and IP-spoofing, etc. In this section we will evaluate the studied authentication schemes to check what protection they provide against possible attacks and for which attack they can’t do anything.

In early IMS security architecture, IP spoofing is main security attack to get authenticated with IMS network because authentication procedure lies in binding of IP address allocated by bearer network with IMS identities, IMPI and IMPU and hence if a malicious user comes to know an IP address of a valid user he can impersonate as a valid subscriber using that IP address to get access to IMS. So the scheme employs that the GGSN
provides protection against IP spoofing [38]. In this way we can say that early IMS security (discussed in section 5.3) does not provide IMS level security, it only provides access to IMS based on the access level security. Eavesdropping can also occur in the network [38] since the communication is not encrypted between UE and IMS network and hence this eavesdropped information can be further used for reply attacks and session hijacking.

In early IMS, lack of mutual authentication mechanism can result in Man in the Middle attack [40], which acts as an extreme attack at network resources and users information. So early IMS authentication mechanism doesn’t provide enough security during authentication procedure.

One of the most powerful features of IMS AKA (discussed in 5.1) and E-IMS AKA (5.5) is mutual authentication through which Man in the Middle attack is avoided. In this way UE knows that it is communicating with the real network and the network knows that the UE establishing a communication channel is a legal entity. Also the communication after initial registration request is done between UE and P-CSCF after establishment of IPSec SA so eavesdropping attack is mitigated but however the initial registration request and subsequent challenge sent by the S-CSCF to the UE in the form of AV is done before SA establishment. If an un-authorized user is somehow able to eavesdrop in the beginning of authentication procedure he/she cannot use the information for replay attack or session hijacking because these schemes implement time concurrency mechanism using SQN and RSN parameters respectively and reuse of these credentials is impossible through the SQN checking mechanism. Both the schemes provide the CK and IK through which the confidentiality and integrity of information exchanged can be maintained, and hence the communication done can’t be eavesdropped easily.

In one pass authentication scheme (discussed in 5.4), there exist more security risk than other schemes. Although it reduces complexity but it results in an increased level of security threats and more vulnerable to some of known attacks. One of the main security flaws in this scheme is the loss of mutual authentication, and any one can impersonate as the network and hence man in the middle attack is most common. There is no mechanism provided for session keys i.e. CK and IK through which the confidentiality and integrity of information exchange can be viable. Due to these security flaws as the information exchanged is not encrypted, there can be active eavesdropping possible by which a malicious user can use the information captured for replay attacks and session hijacking, and also to avoid the replay attacks the SQN mechanism is not present in this scheme.

<table>
<thead>
<tr>
<th>IMS AKA</th>
<th>E-IMS AKA</th>
<th>One-Pass GPRS</th>
<th>Early IMS security</th>
</tr>
</thead>
</table>

49
<table>
<thead>
<tr>
<th>Authentication Parameters</th>
<th>Yes</th>
<th>Yes</th>
<th>No</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual Authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Confidentiality Protection</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Integrity Protection</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Time Stamp</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 6-1: Comparison between authentication schemes based on security parameters

6.2 User Friendliness

User friendliness of any system, device or function means that how the typical or a normal user learns to use it, how much uncomplicated interface it provides for the user to use the services provided by the system. In the term of using a device, it should be designed in such a way that a normal user can easily operate it; it should not have complex functions. In the modern and advance mobile phones, the user interface is designed with a lot of consideration that it should require little efforts from the subscriber to use it to get the different services provided by the network operator.

The user friendliness regarding the UICC based IMS authentication schemes can be further categorized in different aspects to study and evaluate easily. However, we can say that as the UICC is used to get access to the services provided by the IMS, the registration and authentication is performed before the services are available to use. All the functions and credentials relating to the authentication are embedded on the card, so it is the device which reads and extracts the information from the card and almost no or very little effort from the subscriber is required. A subscriber should only power on his/her device containing the UICC and on the prompt, enter a four digit PIN to activate the UICC, however this feature can be disabled. This PIN mechanism is used for security reasons, but greatly impacts the user friendliness of the scheme as process of provision of PIN by the subscriber can have impact on the user friendliness, as the subscriber has to enter the PIN which is not considered as a user-friendly practice. Once the card is activated, the registration/authentication process is activated. All the functions required for authentication are performed between the UE and the network transparently to the user. As the UICC based schemes for authentication requires little or no effort from the user we can easily say that such type of schemes are most user friendly, as all the processes are performed by running the different algorithms stored on the Card and the network database, and the messages exchanged between the entities are hidden from the subscriber.
However, we will elaborate the user friendliness aspects by considering some of other sub criteria, as we can’t say that a scheme is user friendly because it doesn’t take many inputs from the subscriber.

### 6.2.1 Authentication Time

Authentication time is the time taken by any authentication scheme to successfully authenticate the subscriber to the network. For evaluation of authentication scheme fast authentication time is necessary to get a positive response from the subscriber. Authentication time depends on the number of the signaling messages exchanged between the UE and the network. Number of authentication messages are defined as the messages exchanged between different entities during authentication process and helps in the measurement of authentication time. The larger the message to be exchanged during the process, the greater is the time consumed in the authentication.

To scrutinize the authentication schemes based on the number of messages exchanged during authentication procedure, we make use of the SIP and CX messages exchanged (as depicted in the Table 6-2). The table shows the number of signaling messages exchanged between the UE and different entities in the network in the schemes studied earlier (IMS Authentication Schemes). These numbers of messages are taken from the signaling flow diagrams of the respective schemes. The signaling flow for IMS AKA (Figure 5-4), shows that it involves 12 SIP and 8 Diameter messages. While the early IMS security mechanism (shown in Figure 5-5) has 7 SIP messages and 6 Diameter messages, and likewise the E-IMS AKA (depicted in Figure 5-7) has 6 SIP messages and 6 Diameter messages and finally One pass GPRS-IMS authentication (shown in Figure 5-6) has 7 SIP messages and 8 Diameter messages in that order.

<table>
<thead>
<tr>
<th></th>
<th>IMSA AKA</th>
<th>E-IMS AKA</th>
<th>One-pass</th>
<th>Early IMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP messages</td>
<td>12</td>
<td>6</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Diameter messages</td>
<td>8</td>
<td>6</td>
<td>8</td>
<td>6</td>
</tr>
</tbody>
</table>

**Table 6-2: Signaling messages comparison for different authentication schemes**

### 6.3 Simplicity

In the context of evaluation of authentication schemes, it is a basic requirement that the scheme should be simple enough and should not have much impact on the subscriber or the network regarding the complexity and performance. It should be as simple as possible. However, to
accomplish the simplicity the other criterion of security and user friendliness should not be compromised. It is very common observation that whenever an authentication scheme is implemented to be simple then it will not be much efficient in terms of security. But as the main purpose of an authentication scheme is to have a secure system so to attain simplicity on the behalf of security should not be allowed. The authentication scheme should be efficient in terms of security by shielding the system from most common security attacks and should be simple. It is required that the scheme should not have lot of complex computations. The time taken in the authentication of a subscriber should be as little as possible and the functions to compute the authentication data should not be very complex and should not require lot of computations to successfully authenticate. So in this situation a candidate scheme for deployment should have a secure algorithm which should be simple and efficient also.

In this section the simplicity aspects of UICC based authentication schemes will be evaluated on the basis of following sub-criteria to know

### 6.3.1 Performance Impact on System

The performance impact on a system with respect to authentication of a subscriber greatly depends on the algorithm and functions executed for the authentication. It depends on the number of the parameters calculated for a specific authentication scheme, and how complex those functions are, along with the time taken to execute those functions. To have a good impact in terms of performance, the authentication scheme should be simple enough but at the same time this simplicity can have a negative impact on the security of the system.

To evaluate the studied authentication schemes based on the performance parameter, we will consider the computations performed at the system to pave the way for the authentication process.

In IMS AKA (discussed in 5.1) there are five different one-way functions \( f() \) which are used to compute the AV, and then the digest of AUTN and RAND computed using \( PRF() \), which uses MD-5 [37]. We can approximate the time consumed in the computation of \( PRF() \) equal to \( f() \) i.e \( PRF() \approx f() \). So the total time consumed at the network for the computation can be expressed as \( T_{is}=7f() \). Similarly there are two one-way functions used in E-IMS AKA (5.5) for CK and IK represented by 2 \( f() \) along with the four MD-5 represented by 4 \( PRF() \) functions to compute the digest response and http-digest-aka password etc. Then the total time consumed by using the earlier assumption i.e \( (PRF() \approx f()) \) can be represented by \( T_{es}=6f() \). Hence the computation time in IMS AKA is \( 7f() \) whereas computation time of E-IMS AKA is \( 6f() \). Along with the
computational cost there is an additional storage issue in S-CSCF for the AVs calculated in the IMS AKA shown in Figure 5-2, but however these extra AVs fetched to the S-CSCF can greatly reduce the authentication time in terms of computational time as well as the authentication time consumed in the signaling messages, in the subsequent re-authentication requests.

There is almost no algorithmic computations in the early IMS security as well as One Pass GPRS-IMS authentication (discussed earlier in 5.3 and 5.4 respectively). In these schemes only the access level and IMS identities are matched. However, the one pass GPRS-IMS authentication scheme requires a SIP application level gateway (ALG) at the access network to modify the format of Register request; this ALG can add complexity to the access network.

### 6.3.2 Performance Impact on the UE

As stated in the earlier section the performance of the system depends on the type and number of computations performed by the equipment. This computation can be a deciding factor for the evaluation of any system or process.

As stated, there are almost no computations in early IMS security and one pass GPRS-IMS authentication at the UE side other than the signaling messages; hence we can say that this parameter doesn’t have much impact on these schemes. But, however these parameters are of great importance in the other two schemes under consideration as there are lot of computations involved in the process of authentication.

In IMS AKA almost the same computations are performed on the UE side as were performed in the network side. The same five one-way functions $f()$ along with the two $PRF()$ implementing MD-5 algorithm are carried out (discussed in section 5.1). And according to the assumption of the previous section we can say that the computation time at the UE will be $T_{iu}=7f()$ (by using $PRF()\approx f()$). Similarly the computation time in the case of E-IMS AKA will also be same at the UE as compared to the earlier computations at the network side (in section 6.3.1 and discussed in section 5.5), and can be represented by the equation $T_{eu} = 6f()$. Hence from these calculations we can say that IMS AKA is likely to have more computation effort as compared to E-IMS AKA and the other two schemes.
7 Comparison and Discussion

After conducting a systematic evaluation, and as was expected, the results show that every scheme has its own pros and cons, which depends on the parameters used for evaluation. If a particular scheme provides a good security protection, on the other hand it can have serious drawbacks in terms of other parameters like simplicity and user friendliness.

All the schemes evaluated in the preceding chapter provides the same security feature in terms of authentication level as all of them requires UICC and PIN (however it can be disabled) to successfully authenticate the subscriber to the network.

The IMS AKA and E-IMS AKA provide a good security protection by having Challenge-response mechanism instead of exchange of secret keys. In these schemes the mutual authentication is performed through which one of the most common attack i.e. Man in the Middle (M-i-t-M) attack is avoided. In the challenge response mechanism of these schemes there is integrity and confidentiality keys generated, which are used to create the IPsec tunnels and hence the subsequent signaling messages are exchanged in a secure manner. However, the only unprotected signaling is the initial register request. These keys are used to mitigate the eavesdropping attack. Both the schemes provide sequence number checking mechanism in the form of SQN and RSN to avoid session hijacking and replay attacks.

The one-pass GPRS IMS authentication mechanism has serious tradeoffs in terms of security as it does not provide good security protection by lacking the mutual authentication mechanism. For this reason the (M-i-t-M) attack is most common, and an adversary can pretend to be the network or the UE. Also this scheme lacks the session keys CK and IK and by this deficiency the session hijacking is possible as the information exchanged is sent in clear text and can be eavesdropped for fraudulent usage.

The early IMS security does not provide the IMS level security, (described in 5.3.1) it just provides the access level security by having a secure binding between the access level identity i.e. IMSI and the IP address at the bearer level. This scheme is most vulnerable as it does not have mutual authentication capability as well as the integrity and encryption protection in the form of CK and IK, and hence there can be security attacks like eavesdropping and session hijacking. Also this scheme lacks the sequence number checking mechanism means the session can be hijacked or a replay attack can take place.

All the schemes under observation exhibit the same quality in terms of re-authentication and timeout mechanism (specified in the section 6.1.2) as
all of them employ SIP register request to authenticate itself to the network.

To compare the evaluated authentication schemes in terms of user friendliness we studied the parameter i.e. authentication time, the time it takes to successfully authenticate the subscriber. The E-IMS AKA (discussed in section 6.2.1) takes the minimum time in authentication as it requires minimum number of messages to be exchanged for a successful authentication.

To evaluate the schemes under the criterion of simplicity we studied them in terms of performance impact on the system and the UE respectively. As it is a common observation that to reduce the complexity or in other words to have a simple authentication scheme which has less impact on the performance of a system, the security can be compromised. Trying to achieve simplicity can result in some security impacts.

The early IMS and One Pass GPRS IMS (studied in 5.3.1 and 5.4) authentication does not have much impact on the performance of the system as well as the UE (evaluated in 6.3.1 and 6.3.2) as they require little or no computations for successful authentication. However for IMS AKA and E-IMS AKA (studied in 5.1 and 5.5) the evaluation in terms of simplicity (discussed in 6.3) shows that E-IMS AKA requires less effort than the IMS AKA and hence it is simpler. To consider the security parameter of timeout and re-authentication IMS AKA is better as it computes an array of authentication vectors which can be subsequently used in case of time out. Hence, it greatly reduces the computation time whereas the E-IMS AKA has to follow the whole procedure which can have a negative brunt over the overall simplicity parameter.
8 Conclusion

This thesis work is an evaluation of UICC based authentication schemes for IMS that can be used as authentication and access control solutions for IMS in FMC multi-access environment. A detailed study of UICC based IMS authentication schemes was carried out, which are regarded as candidate schemes to be implemented in IMS based FMC. The goal of this evolution is to propose a scheme that can be employed in IMS based FMC in multi-access environment.

The schemes that were evaluated are IMS AKA, E-IMS AKA, One-pass GPRS-IMS authentication and Early IMS authentication, where the first three schemes relies on IMS specific module ISIM or USIM on UICC and the last one is based on traditional SIM module on UICC.

On the basis of the study, these schemes were evaluated by considering security, user friendliness and simplicity. These parameters were further categorized as authentication level, timeout and re-authentication and security attacks for security. Regarding user friendliness the parameter that was considered for evaluation was authentication time. The last parameter that was considered was simplicity, which was evaluated on the basis of performance impact on system and UE.

From the detailed study of the authentication schemes and analysis (chapter 7) we came to know that E-IMS AKA is good in terms of security as it provides almost same security protection like IMS AKA by having mutual authentication, session keys and sequence number mechanism. Also this scheme is better in terms of authentication time (discussed in 6.2.1), as it has less number of signaling messages exchanged in a successful authentication process. But has drawbacks in the re-authentication and timeout mechanism at the UE and the network, as a lot of computations are done on every re-authentication request.

The one-pass GPRS IMS authentication mechanism is the most competent process in terms of simplicity but has serious tradeoffs in terms of security as it does not provide good security protection by lacking the mutual authentication capability, not providing session keys and sequence number mechanism through which replay attacks and session hijacking are most common to occur [44].

The early IMS security mechanism is the most threat full procedure and doesn’t provide IMS level security, it just provides security in IMS domain by binding the IMS level entities with the bearer level identities. Hence, it only provides the bearer level security. But it can be used for a specific time in the interim implementation of IMS.

So, after going through the detail study and evaluation, it is recommended that IMS AKA based on ISIM module embedded on UICC is the most thriving candidate to be implemented in the multi-access FMC environment based on its qualities in terms of security, user-friendliness.
and simplicity. As stated earlier the IMS AKA and E-IMS AKA exhibit same qualities in terms of parameters based on security and user-friendliness, but the IMS AKA is better than E-IMS AKA in terms of simplicity. In this scheme the performance impact on the system and UE is not better for a single authentication as compared to E-IMS AKA but it greatly reduces the computation time on UE and at the system by having the AV mechanism which can be used in subsequent re-authentication request without any additional computational time and in this way a greater level of security is also achieved. However, due to lack of support of UICC by majority of the UE supported by IMS, it is recommended that there should be some sort of special purpose devices to be used through which the UICC can be supported.
9 Future Work

This section proposes the most of the flourishing proposals to be considered. These can be design and implementation of an authentication scheme in which we can have a good and enhanced level of security and most efficient in terms of simplicity. This can be done by considering the AV mechanism to be implemented in the E-IMS AKA.

Also, due to the scope of the thesis a lot of potential non SIM based candidate schemes were not evaluated, which can be done. However, efforts will be made with the help of my thesis supervisor to propose a proficient and secure authentication mechanism that can be employed in the FMC environment.
Reference


[13] ETSI TS 101 348 Digital cellular telecommunications System (Phase 2+); GPRS ; internetworking between PLMN supporting GPRS and PDN (GSM 09.61 V7.2.0 release )


[22] IMS Architecture and Session Control Functions, white paper, Newport networks.


[24] Parameshwar and Reece, Advanced SIP Series: SIP and 3GPP, Award Solutions, Inc.


[27] 3GPP TS 23.003 Release 7 Numbering, addressing and identification.


[29] RFC 3261 “SIP: Session Initiation Protocol”.


[34] MOBICOME Deliverable 4.1 a IMS Authentication and Access Control Solutions.
[35] Ja'afer AL-Saraireh & Sufian Yousef, Extension of AKA protocol for UMTS, NIST.


[38] 3GPP TR 33.978 3G Security aspects of early IMS version 7.0.0 Release 7.

[39] Peter Howard, GSM and UMTS security presentation, Vodafone Group R&D.

[40] Dubravko Priselac, Miljenko Mikuc “Security risk of pre-IMS AKA access security.


[43] 3GPP TS 24.228 UMTS Signaling flows for the IP multimedia call control based on SIP and SDP, Stage 3.

[44] Lin; Chand; Hsu; Wu; One-pass GPRS and IMS authentication procedure for UMTS, IEEE Communications journal, Volume 23,2005.