UMTS Authentication and Key Agreement

- A comprehensive illustration of AKA procedures within the UMTS system

Graduate Thesis

Sivilingeniør Degree
Information and Communication
Technology

By
Jon Robert Dohmen
Lars Sømo Olaussen

Grimstad - Norway, May 2001

Abstract

This report will give information on the 3rd generation mobile communication system, UMTS, its Authentication and Key Agreement (AKA) procedures and security aspects. It will also describe the 'UMTS AKA Illustrator' which is an animation program we have created to explain the AKA procedures.

The AKA procedure is the essence of authenticating a user to the network and vice versa. This is possible due to the pre-shared secret key K stored in the Authentication Centre (AuC) and in the UMTS Subscriber Identity Module (USIM). The other parameters are derived from this key.

During an AKA procedure, messages with parameters to be confirmed by the User Equipment (UE), are delivered from AuC. Such parameters are joined together in an Authentication Vector (AV). The AV is delivered to the Core Network, which distributes parts of this AV through the access network to the UE. The UE must then perform some calculations to match this challenge. The result of the UE is sent back and checked against the AV where it originated. If the result matches, then the authentication is successful. If the result fails some other procedures are activated to correct the problem.

The above description is successfully animated using Flash technology. This animation we have called: 'UMTS AKA Illustrator' and is the result of a literature study of 3GPP specifications. This illustrator is developed for making the AKA procedures easier to understand for people without the deeper knowledge of UMTS. The illustrator can be used as a stand-alone application for educational purposes, with easy web access on multiple platforms.

AKA procedures in UMTS have increased security compared with GSM. The new feature of two-way authentication eliminates the problem with false basestations. This is a very important security improvement.

Even though the security has improved in some areas, there are still security features that should be improved. It is not sufficient to just require integrity protection on signalling messages. All messages should be integrity checked, but indirectly by requiring confidentiality protection together with integrity.

Acknowledgements

The making of this thesis would not have been possible without the help and guidance of Telenor R&D Agder. We send a special thanks to Research Manager Geir M. Køien and Senior Engineer Runar Langnes.

- I would like to dedicate this report to my father, Jan Håkon, for being the best a father can be and who always has been my mentor through all my studying. Best wishes for the future.

Jon Robert

- A mes parents de m'avoir donné la vie et à Lattja de lui avoir donné une sense.

Lars

Finally, we would like to acknowledge the efforts of our colleagues and fellow students for their contribution.

Preface

This preface chapter enables the reader to get an overview of main aspects of the thesis. Here you can find some short information about; the security trend in UMTS, assignment requirements and description, methods and tools that have been used.

Security and development of 3G systems

Wireless systems have achieved phenomenal penetrations and now challenge fixed line communications. Bandwidth hungry applications have set new standards for what is expected of wireless communication. Based on these new trends the demand for a complementarily to the second-generation systems, like GSM, PDC, DECT and others, is due. UMTS has consequently been developed all the way through as a joint effort of many companies and telecom operators. UMTS is a proof of the merging of packet and circuit switched systems to give the user more flexibility. All of these changes, demand increased security features that are satisfactory and practical.

This rapid shift is causing a change in the way; telecom operators, equipment, manufacturers and service providers operate. Alliances are now taking place, which will result in a few global operators and several niche players. The need for secure solution maintaining integrity, confidentiality and protect against fraud will be essential. Especially since UMTS will become world widespread. One must keep in mind that such security solutions must also be upgradeable to keep up with computing power of the future, which potentially can be used to break down today's algorithms.

We are proud to be able to enlighten some of these security issues by gathering information from UMTS specifications for this Postgraduate thesis. We are also very pleased to be associated with a university community and sponsoring companies of Agder University College, Grimstad. We hope our effort will capture the security architecture of UMTS wireless communication development today.

Why is security in UMTS so important?

Since the beginning of second-generation wireless systems, there has been a discussion around security solutions. A security solution was not implemented from the beginning in GSM, but more or less as an optional feature for the telecom operators to implement. From a users perspective some questions always remains uncertain, regardless of what is being claimed by manufacturers and operators; -How secure are wireless systems? -How do they 'actually' work? -Do users have any influence or control over these mechanisms?

To reduce the amount of uncertainty in third generation systems, Telenor R&D Agder (Telenor FoU, Grimstad) decided to use the opportunity of using students to make an Illustrator showing principles of authentication in UMTS. The information around this security topic within UMTS is not widely spread or understood, we therefore believe a graphical representation will illustrate this better than any other means at the moment. This Illustrator will therefore be used to educate and brief people about Authentication and Key Agreement in UMTS. But first let us have a look at requirements and assignment description before we go further into the world of wireless security.

Thesis title

UMTS Authentication and Key Agreement
- A comprehensive illustration of AKA procedures within the UMTS system

Graduate thesis at Agder University College

There are set two main issues here that are meant to be sort of guidance for this project. Firstly we would like to describe the Postgraduate thesis requirements set by the Agder University College. Secondly we present the assignment description made by Telenor R&D department in Grimstad and us.

Graduate thesis requirements

This thesis is performed at Agder University College, Department of Technology, Institute of Information and Communication Technology (ICT), Norway. As a general rule all postgraduate thesis must at least fulfil some standard requirements. First and foremost the thesis shall give an independent deepening within a central sphere of the ICT Master study itself. Secondly there is a formal requirement designed by the university college, which is described below.

The text below is a translation from Norwegian into English and describes the main contents of the subject code (IKT6400). The text is intended to be a kind of guidance and not any absolute requirement set by Agder University College:

"The postgraduate thesis assignment is a independent section of work within a central sphere of the study. The work shall have a character of research i.e. the thesis must have elements of new knowledge or methods. Pure design, development, programming tasks should be avoided. Normally a preliminary study of 2 weighted points in size is performed. The preliminary study can be; literature search, preliminary exploration search, mapping of the status on the current topic or an intensive training period of methods or techniques. The postgraduate thesis assignment shall be put into a report that describes the problem, results and the work. Prototypes and/or other products that are developed could enter as a part of the solution. The assignment shall also be orally presented in a presentation."

Literature for the thesis is chosen in coherence with the subject supervisor. The supervisor will be available for frequently consultancies or meetings.

The general evaluation criteria are given on the basis of a written report on the subject, any products or prototype that is part of the postgraduate thesis, and a final presentation. The subject supervisor and external sensor evaluate the thesis. The director of studies is responsible for the subject (IKT6400).

The thesis also sets four milestones that every project at the ICT study has to uphold to graduate. They are as follows: assignment description date is due 2. February 2001, report delivery date is due 28. May 2001, poster delivery date is due 5. June 2001, presentation date is 14. June 2001.

Assignment description

The plain text of the assignment of this postgraduate thesis is quoted below. This is the original description and there have been no changes during the project time period:

"Telenor Research & Development branch office in Grimstad, wants to use an educational Illustrator to demonstrate how UMTS Authentication and Key Agreement (AKA) procedures are to be implemented. UMTS stands for Universal Mobile Telecommunications System. It is the 3rd generation mobile telecommunications standard that will be implemented worldwide within the next few years. It offers both circuit and packet switched data transfer with speeds up to 2 Mbps.

AKA are the procedures taking place between the different nodes in the UMTS network. They are used to authenticate both user and network and to establish keys used for confidentiality and data integrity. The Illustrator should show how the different entities involved interact and let the viewer see different occurrences where the AKA procedures are taking place.

To do this we want to make an interactive computer animation that lets the user see and control the progress of the AKA procedures. Both the different nodes and entities in the UMTS system and the signals going between them will be represented by illustrations and animations. This animation will be represented in a format that can be reached by most people with today's technology. Some knowledge of UMTS will be required to understand the Illustrator.

A well-extracted documentation with material from several relevant technical specifications will be accompanied with the animation. This is intended for further studies about UMTS AKA, but with a more easily comprehended approach than the formal technical specifications. In addition we will give an evaluation of the suitability of the UMTS AKA procedures."

Report structure

Our main emphasis in this report has been structure and explanatory figures. First of all it is important to make the readers who are not familiar with UMTS a chance to figure out how this works by reading the introduction chapter. Nonetheless it is clearly favourable to have some knowledge about the GSM system. To understand Authentication and Key Agreement procedures one should understand the functions of the components involved in the system, and that is gained by reading the chapter about UMTS. In the next chapter a general description of security architecture is given to understand the main concept behind UMTS security. The essential chapters that explain AKA procedures and AKA algorithms are chapter 5 and chapter 6. At the end there are a few chapters discussing and concluding some of the security features, these are chapter 9 and chapter Conclusion.

Sivilingeniørstudent, Jon Robert Dohmen
Sivilingeniørstudent, Lars Sømo Olaussen

Agder University College
Grimstad, Norway
May 2001

Contents

1 Introduction

The introduction chapter enables the reader to easily and clearly get an overview of the thesis main aspects. The chapter gives short information about; assignment description and requirements, UMTS overview, AKA procedures, AKA Illustrator, methods used and report structure.

1.1 UMTS overview

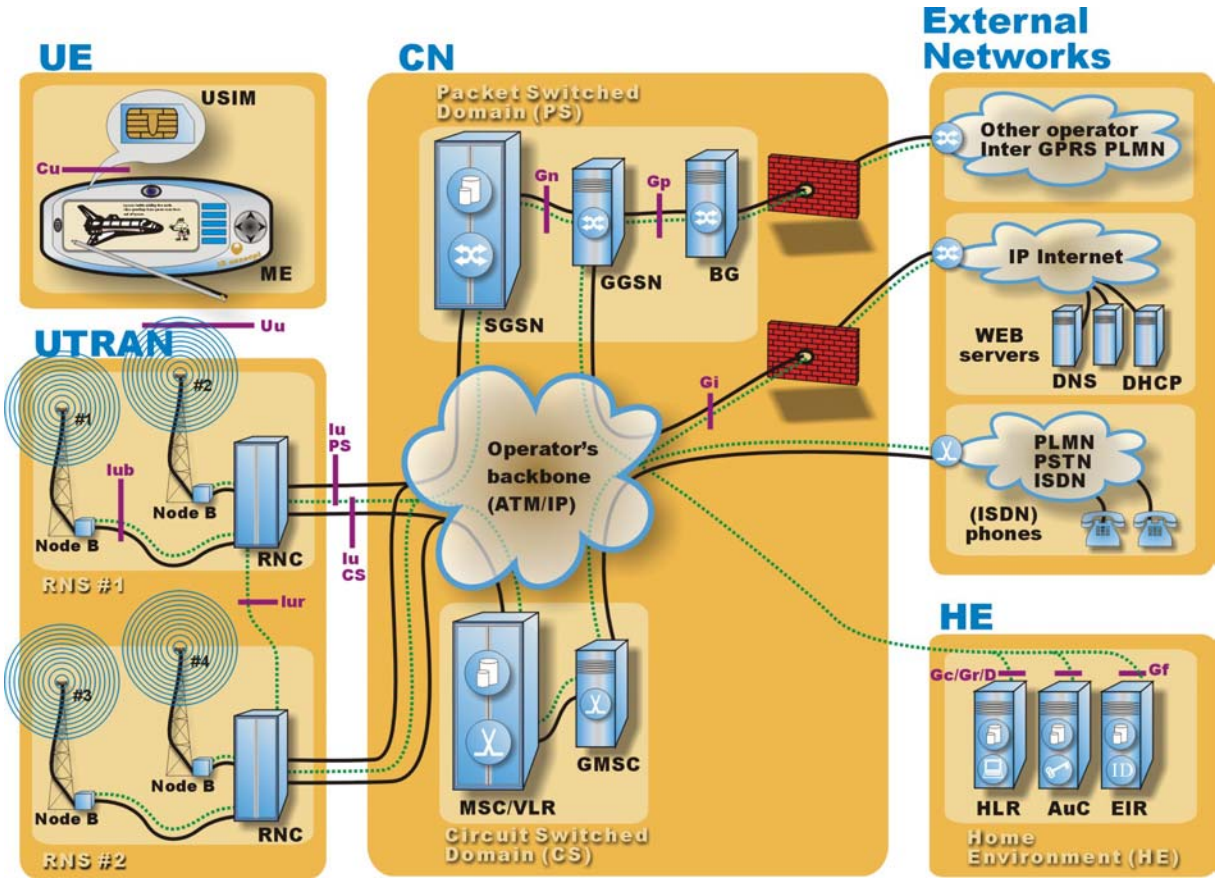

Figure 1 Overview of the UMTS system.

1.2 UMTS AKA overview

AKA are the procedures that take between the user and network to authenticate themselves towards each other and to provide other security features such as integrity and confidentiality protection.

The Core Network (CN) initiates the authentication procedure towards the USIM on behalf of the users' Home Environment (HE). The user accepts the identity of the CN and the network accepts the user. Then integrity and confidentiality protection is activated between the UE and RNC.

1.3 The UMTS AKA Illustrator

The UMTS AKA Illustrator is a Flash-animation that shall give a visual representation of the AKA procedures in UMTS. The animation is an interactive program that lets the user see and control the progress of these procedures. Each node within the UMTS system exchange messages at protocol

level and can be viewed as animated radio waves or bit streams. Whenever a 'signalling action' is performed these appear as numbered messages on the screen and hence easily followed by the user.

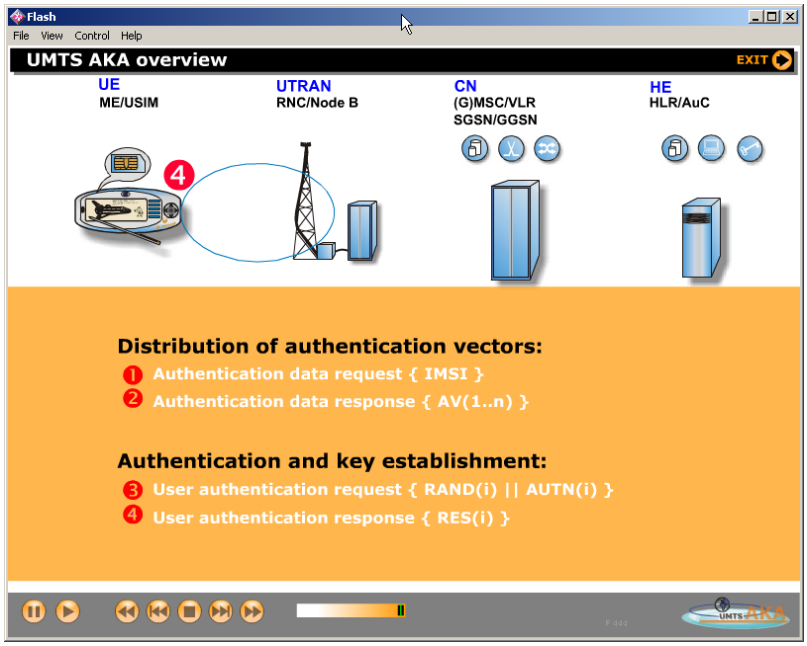

Figure 2 Snapshot of the illustrator

2 Methods

The assignment description gives some natural limitations as whereas who is going to read this thesis report and who is going to use the AKA Illustrator. Some limitations are due to our unfamiliarity with Flash 5 and limited programming skills.

Regular meetings were arranged to keep track of the progress in the project. Meetings were held 19. January, 2. Mars, 30. Mars, 2. May and 21. May at Telenor R&D Agder.

First we would like to emphasis that this report has the purpose of covering both users of the AKA Illustrator and the formal demands of a thesis at Agder University College. This limits us to write a balanced structured report satisfying all users of this report.

To master an unfamiliar program such as Flash 5 we had to use relatively much time to reach an acceptable level of skill to produce any useful animations. This could have limited the result e.g. the extent of using fancy graphics and other features that would be possible if we where at a higher user level.

Most of the documentation is gathered from 3GPP collection of Release-99 specifications, which can be downloaded from the worldwide website; http://www.3gpp.org/. The most frequently used specifications have been; 3GPP TS 33.105 v360 (Cryptographic Algorithm Requirements), 3GPP TS 33.102 v370 (Security Architecture), 3GPP TS 33.120 v300 (Security Principles and Objectives), and some MILENAGE documents that are intended for internal use only. For UTRAN two versions of a book on WCDMA for UMTS by Harri Holma and Antti Toskala [1] have been helpful.

The specifications have been to a great extent throughout the specification that it seems pointless to add references at every other sentence. Instead the list of references shows what documents have been used.

3 UMTS

UMTS, Universal Mobile Telecommunications System is a third generation (3G) system for global mobile communication. From first generation (analogue) systems like NMT through second generation systems like GSM, the mobile industry have moved from simple, low quality voice services to high quality, high capacity voice and data communication services.

The project was developed among others by ETSI, the European Telecommunication Standards Institute and was started to increase the data rates from GSM, give new and more services to the end users and provide a truly global system. The 3rd Generation Partnership Project (3GPP) is responsible for the development of the UMTS system.

UMTS provides both packet and circuit switched connections, with packet switching giving the highest data rates, up to 2Mbps per user.

This chapter gives a brief introduction to the UMTS system areas such as services, nodes and interfaces.

3.1 Services in UMTS

UMTS will offer both packet and circuit switched connections with speeds up to 384kbps in the CS domain and 2Mbps in the PS domain. This offers a new set of services to mobile users only seen in fixed telephone networks and on the Internet. These services will include video telephony (video conferencing), higher transfer rates and high (CD) quality sound on the terminal. Another feature, introduced with General Packet Radio Service (GPRS) is to be 'always connected' to the Internet. UMTS will also give better location information and thus giving more and better location based services.

3.2 User Equipment

The User Equipment (UE) is the user end of the UMTS network. This part is likely to be made in the most numbers and it's development will in some ways guide which services and applications will be made available. The price has to be low to quickly enable users to buy new UMTS ready equipment. This is achieved by standardising the radio interface and putting all user intelligence on SmartCards.

3.2.1 Terminals

A phone is no longer just a phone, with new data services being offered, the name have been changed to terminal. The major manufacturers have showcased different concept terminals, but few have actually gone into production. Even though the concept terminals all differ in size and design, all of them have larger screens and fewer buttons compared to 2G phones. This is mainly due to the increase in use of the terminal, for more and more data services, and the terminal is thus becoming combinations of mobile phone, modem and palmtop computer.

The terminal offers three interfaces. The two main interfaces are the Uu interface that defines the radio link (Wideband Code Division Multiple Access interface). It will take care of all the physical connection to the UMTS network. The second is the Cu interface between the terminal and the UMTS IC Card (UICC). This interface follows the standard format for SmartCards.

Even though the manufacturers of terminals have many different design ideas on the terminals, they have to comply with a minimum set of standard definitions, allowing users to get access to some basic functions in the same way using different terminals [14].

These standards comprise:
- Keypad (physical buttons or virtual buttons on a screen)
- Registration of new password

- Changing of PIN codes
- Unblocking of PIN/PIN2
- Presentation of IMEI
- Handling of supplementary services
- Call control

It is up to the terminal developers to decide the rest of the user-terminal interface and the user will probably choose it's terminal based on two criteria if the trend from 2G mobiles is prolonged, namely design and interface. The interface is a combination of the size and information given by the (touch)-screen, buttons and menus.

3.2.2 UICC

The UMTS IC Card (UICC) is a SmartCard and as hardware concerned merely interesting as how much memory and what processor speeds it can provide. The USIM application is run on the UICC.

3.2.3 USIM

In the GSM system, the SIM card held the personal (subscription) information hard-coded onto the card. This has changed and in UMTS the UMTS Subscriber Identity Module is placed as an application on the UICC. This allows for more applications and/or keys/electronic signatures for other purposes stored alongside the USIM on the UICC (e.g. secure banking transactions access codes). It also gives the opportunity to have multiple USIMs on the same UICC, thus providing access to multiple networks.

The USIM contains functions and data needed to identify and authenticate the subscriber in the UMTS network. A copy of the subscriber's service profile may also be stored.

The user should authenticate himself to the USIM by entering a PIN code. This is to make sure that the access to the UMTS network is granted the real user. The network will provide services to whoever is using the terminal based on the USIM identity claimed, not the user.

3.3 UMTS Terrestrial Radio Access Network

The UMTS Terrestrial Radio Access Network (UTRAN) is the link between the user and the CN. It consists of all elements to provide UMTS communications over the air and control of such. The UTRAN is currently the only Radio Access Network defined, though satellite communications have been discussed as an alternative. Another possible radio access network is HIPERLAN, a high-speed wireless LAN technology under development.

The UTRAN is defined between two interfaces. The Iu interface between the UTRAN and CN, that is divided into two parts, the Iu PS for the packet switched domain and the Iu CS for the circuit switched domain; and the Uu interface between the UTRAN and the User Equipment.

Between these interfaces are two nodes, the RNC, RNC, and the basestation, Node B.

3.3.1 RNC

The Radio Network Controller (RNC) is responsible for one or more basestations and controls their radio resources. It is also the service access point for the services the UTRAN provide the CN. It is connected with the CN with two connections, one to the packet switched domain, the SGSN, and one to the circuit switched domain, the MSC.

Another important job of the RNC is confidentiality and integrity protection. After the authentication and key agreement procedures have taken place, the subscriber's integrity and confidentiality keys are placed in the RNC. These are then used together with the 'built-in' security functions, f8 and f9.

A RNC can have multiple logical roles depending on what node it serves. A user will be connected to a Serving RNC. When the user roams and gets to another RNC, a Drift RNC will take over control over the radio resources of the user, but the Serving RNC will still handle the user's connection

towards the CN. The last role a RNC can have is 'Controlling'. Each Node B has at Controlling RNC that is responsible for its radio resources.

3.3.2 Node B

The basestation have been named Node B in UMTS and its job is to perform the physical radio connection between the terminal and itself. It receives signals over the Iub interface from the RNC and converts this to radio signals over the Uu interface. It also performs some basic Radio Resource Management operation as the 'inner loop power control'. This is a feature to prevent the near-far problem; that is that if all terminals send with the same power, the terminals closest to the Node B will drown the signal from the terminals far away. The Node B checks the power received from the different terminals and tells them to reduce or increase the power so the Node B will receive the same amount of power from each terminal.

3.4 Core Network

The Core Network (CN) is divided into two parts, packet switched (PS) and circuit switched (CS) domains. The PS domain offers data services for the user by connections to the Internet and other data networks, and the CS domain offers 'standard' telephone services to other telephone networks.

The nodes in the CN are interconnected by the operator's backbone, typically linked by high-speed network technologies like ATM.

3.4.1 SGSN

The Serving GPRS Support Node (SGSN) is the main node of the packet switched domain. It is connected to UTRAN by the Iu PS interface and to the GGSN by the Gn interface. The SGSN is responsible for all packet switched connections for the subscriber. It holds two types of subscriber data, subscription information and location information.

Subscriber data stored in the SGSN:
- International Mobile Subscriber Identity (IMSI)
- Temporary identities (P-TMSI addresses)
- Packet Data Protocol (PDP) addresses

Location data stored in the SGSN:
- Routing area of the subscriber
- VLR number
- GGSN addresses of every GGSN that have active connections

3.4.2 GGSN

Gateway GPRS Support Node (GGSN) is a SGSN that is interconnected to other data networks. All data communications go through a GGSN between the subscriber and external networks. As with the SGSN it holds both two types of data, subscriber information and location information.

Subscriber data stored in the GGSN:
- International Mobile Subscriber Identity (IMSI)
- Packet Data Protocol (PDP) addresses

Location data stored in the GGSN:
- Address of current SGSN the subscriber is connected to

The GGSN is connected by the Gi interface to the Internet and by the Gp interface to the Border Gateway.

3.4.3 BG

The Border Gateway (BG) is a gateway between the Public Land Mobile Network's (PLMN) packet switched domain and external networks. The function of this node is quite similar to a Internet firewall, to keep the subscriber within the network secure for external attacks.

3.4.4 VLR

The Visitor Location Register (VLR) is the serving networks 'copy' of the subscriber's Home Location Register. The subscriber data needed to offer the subscriber it's services are copied from the HLR and stored here. Both the MSC and the SGSN have VLRs connected to them.

The following data is stored in the VLR:
- International Mobile Subscriber Identity (IMSI)
- Mobile Station International ISDN Number (MSISDN)
- Temporary Mobile Subscriber Identities (TMSI) if any
- Current Location Area (LA) of the subscriber
- Current SGNS node the subscriber is connected to

In addition the VLR may hold more information about what services the subscriber is assigned.

Both the SGSN node and the MSC are implemented as one physical node with the VLR and thus named VLR/SGSN and VLR/MSC.

3.4.5 MSC

The Mobile-services Switching Centre (MSC) is in charge of the circuit switched connections between terminals and networks. It performs all of the switching and signalling functions for the subscribers in its coverage area. The functionality of the MSC in UMTS is similar to the functions of the MSC of GSM, but with increased capabilities.

The circuit switched connections goes over the Iu CS interface between UTRAN and MSC. From there they go through GMSC to external networks.

3.4.6 GMSC

Some or all of the MSCs can be Gateway MSCs (GMSC). A GMSC is responsible for performing the routing functions to the location of the mobile equipment. When external networks tries to connect to the PLMN of an operator, a GMSC receives the connection establishment request and asks the HLR of the current MSC of the user. It then routes the call to this MSC.

All circuit switched connections that are not terminated within the same operator are connected through a GMSC to the external networks.

3.5 Home Environment

The Home Environment (HE) holds service profiles of the operator's subscribers. It also provides Serving Networks with subscriber and billing information needed to authenticate the users and charge them for the services offered. Both what services offered and what services blocked are listed here.

3.5.1 HLR

The Home Location Register (HLR) is a database in charge of the management of mobile subscribers. A mobile network may consist of many HLRs, depending on the numbers of mobile subscribers, the capacity of each HLR and the internal organisation of the network.

The database consists of the International Mobile Subscriber Identity, at least one Mobile Subscriber ISDN Number (MSISDN) and at least one Packet Data Protocol (PDP) address. Both IMSI and the MSISDN numbers can be used as keys to access the other information stored. To be able to route and charge calls, the HLR also holds information on which SGSN and VLR that are

currently in charge of the subscriber. Other services offered, such as call forwarding, data rates and voice mail are also listed in together with service restrictions, like roaming limitations.

The HLR and AuC are two logical network nodes but often implemented at the same physical node. The HLR holds all the information about the user and subscription. Namely billing information, which services that are offered and rejected and call forwarding information. But also the important information about which VLR and SGSN the user is currently attached to.

3.5.2 AuC

The AuC holds all the data needed for authentication, ciphering and integrity for each user. It is associated with an HLR and they are implemented as one physical node. This makes it easy to integrate the databases, but these should be kept strictly separate, and the AuC should never give out any information to the HLR other than AVs.

The AuC stores the pre-shared secret key K, for each subscriber in addition to all key-generating functions, f0-f5. It generates the AVs, both in real time when requested by the SGSN/VLR or when the processing load is low, to generate spare AVs.

3.5.3 EIR

Equipment Identity Register (EIR) is responsible for storing the International Mobile Equipment Identities (IMEI). This is a unique identity to all terminals. The database over IMEI numbers is divided into three parts, white, grey and black lists. The white list contains all the IMEI numbers that can be granted access to the network. A terminal is placed in the grey list when it is being watched or traced in the network, and if it's to be completely blocked from access, it's placed in the black lists. When a terminal is reported stolen, its IMEI will be placed in the black list and thereby be denied access. It can also be used to keep specific series of terminals out of the network if they are not functioning according to specifications.

3.6 External Networks

The external networks are not a part of the UMTS system itself, but it's necessary to offer inter-operator communications. The external networks can be either different telephone networks, like public land mobile networks (PLMN), public switched telephone networks (PSTN) and ISDN, or data based networks, like the Internet. The packet switched domain connects to the data networks, while the circuit switched network connects to the telephone networks.

3.7 Interfaces

The roles of the different nodes in the network are merely defined through the different interfaces. These are then defined strict so different manufacturers can interconnect their different hardware.

3.7.1 Uu

The Uu interface is the WCDMA, Wideband Code Division Multiple Access, radio interface defined for UMTS. The interface is between the Node B (basestation) and the terminal.

3.7.2 Iu

The Iu interface connects the CN and the UTRAN. It consists of three parts, the Iu PS for the packet switched domain, the Iu CS for the circuit switched domain and the Iu BC for the broadcast domain. The CN can connect both to multiple UTRANs for both Iu PS and CS interface. But the UTRAN cannot connect to more than one CN access point for each of them.

4 UMTS security architecture

The security architecture in UMTS is based on three security principles:
- Authentication
- Confidentiality
- Integrity

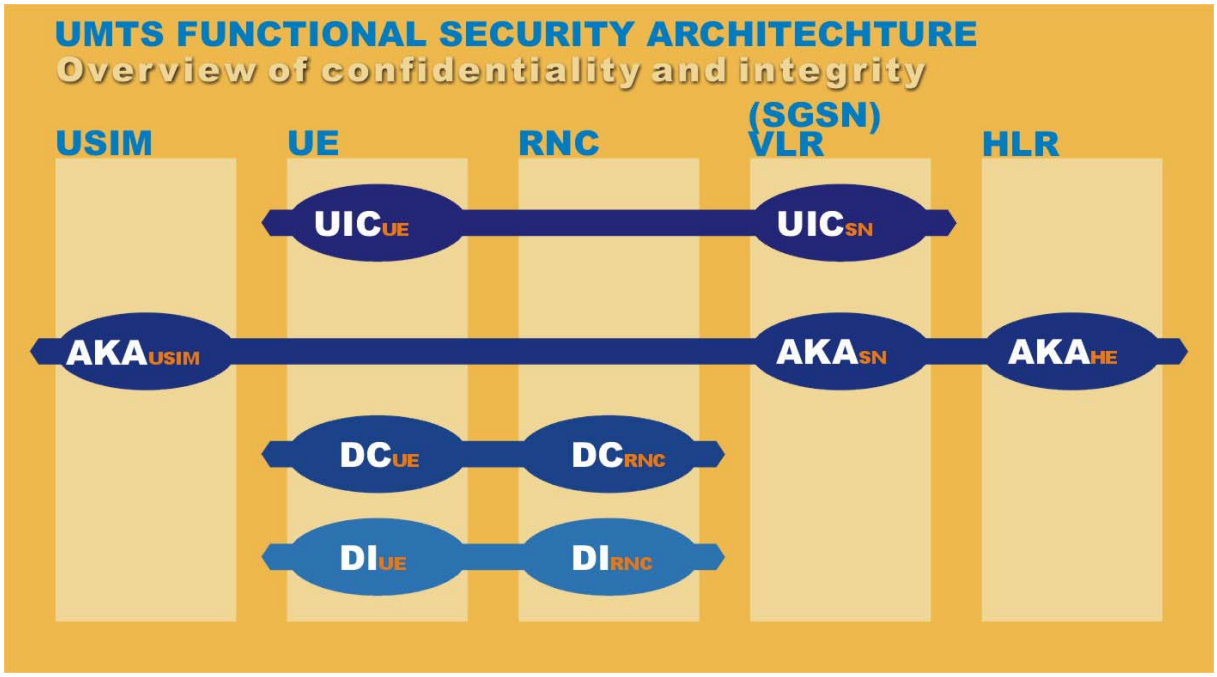

Figure 3 Overview of the UMTS security architecture

4.1 Authentication

Authentication is provided to assure the claimed identity of an entity. A node that wants to authenticate itself to someone has to show it's own identity. This can be done either by showing knowledge of a secret only the nodes involved knows; or by letting a third party that both nodes trusts, vouch for their identities.

The use of authentication is very important when going from just voice telephony, where the actual voice of a person can be some sort of authentication, to more data communication where no human involvement is required.

Authentication in UMTS is divided into two parts:
- Authentication of the user towards the network
- Authentication of the network towards the user

Both these procedures take place within the same message exchange between them. This is a so-called 'one-pass authentication' reducing messages sent back and forth. After these procedures the user will be sure of that the network it is connected to is served by or trusted to serve on behalf of it's own home network. And the network will be sure that the claimed identity of the user is true.

Authentication at this layer is needed for the other security mechanisms as confidentiality and integrity. For the serving network it is very important to know the real identity of the user so it can be sure it will be paid for the services it is offering. The user on the other hand wants the authentication to make sure that the services user pays for is delivered.

4.2 Confidentiality

Confidentiality is to keep information secured from unwanted parties. With more and more people using the terminals for both personal and business calls (e.g. online services like banking) the need for keeping the communication secure grows rapidly.

Confidentiality in UMTS is achieved by ciphering communications between the subscriber and the network and by referring to the subscriber by temporary (local) identities instead of using the global identity, IMSI. The differences are shown in the Figure 3. Ciphering is carried out between the subscriber (USIM) and the RNC, RNC, and user confidentiality is between the subscriber and the VLR/SGSN.

The properties that should be confidential are:
- The identity of the subscriber
- The current location of the subscriber
- User data (both voice and data communications should be kept confidential)
- Signalling data

If the Serving Network does not support user data confidentiality, the subscriber should be informed and have the opportunity to refuse connections.

4.3 Integrity

Sometimes a message's origin or contents have to be verified. Even though it might come from a previously authenticated party, the message may have been tampered with. To avoid this, integrity protection is necessary. The message itself might not even have to be confidential; the important thing is that it's genuine.

The method for integrity protection in UMTS is to generate stamps to be added to messages. The stamps can only be generated at the nodes that know the keys derivate of the pre-shared secret key, K. They are stored in the USIM and the AuC. It is very important to offer integrity protection, especially since the serving network often is operated by another operator than the subscriber's own operator.

The property that should be integrity protected is:
- Signalling messages

At the physical layer, the bits are integrity checked by CRC checksum, but these measures are only included to achieve bit-error free data communications through the air, and are not equivalent to transport level integrity.

5 Authentication and Key Agreement

Authentication and Key Agreement (AKA) are one of the most important features of the UMTS system. All other services depend on them since no higher-level services can be used without authentication of user.

Authentication:
- Identifying the user to the network
- Identifying the network to the user

Key agreement:
- Generating the cipher key
- Generating the integrity key

When the Authentication and Key Agreement is performed:
- Integrity protection of messages
- Confidentiality protection of signalling data
- Confidentiality protection of user data

The Authentication and Key Agreement procedures take place in the USIM, SGSN/VLR and the HLR/AuC. Since the Serving Network is divided into Packet Switched (PS) and Circuit Switched (CS) domains, VLR/SGSN means either the SGSN/VLR node in the packet switched domain or the VLR/MSC node in the circuit switched domain. The authentication procedures are performed in the same way in both domains, so there is no need to make a distinction between these. There are no common information base between the SGSN/VLR and VLR/MSC, except from the Home Environment, so the AKA procedures take place independently in both PS and CS domain.

To simplify the illustrations, VLR/SGSN is used to represent either the SGSN/VLR or MSC/VLR node.

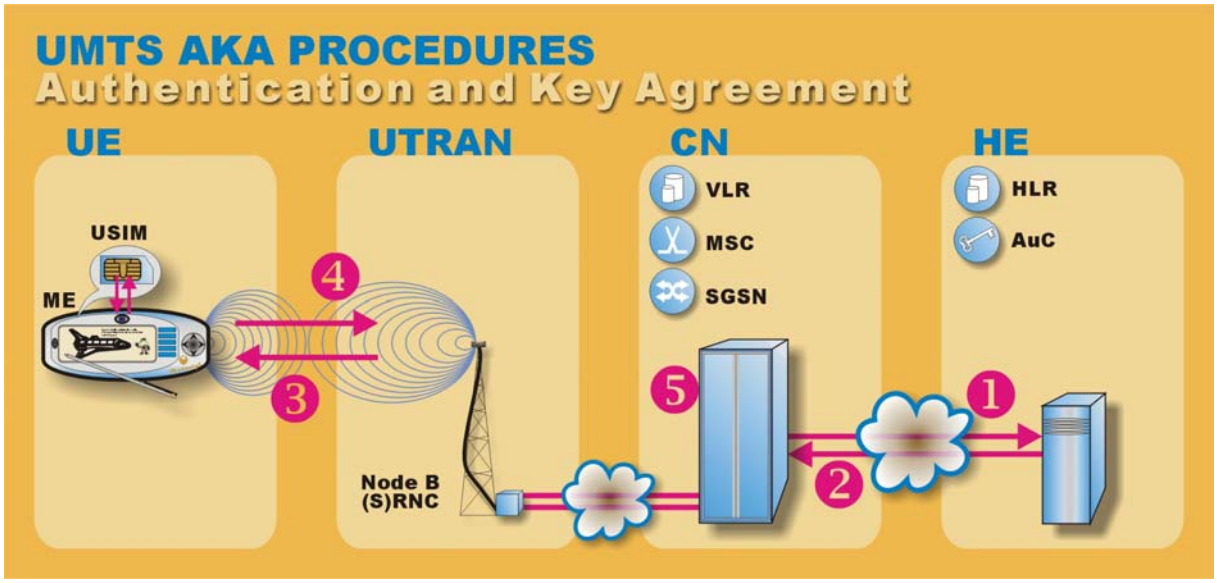

Figure 4 Overview over Authentication and Key Agreement.

5.1 Normal AKA procedure

Authentication and key agreement is managed by the VLR/SGSN that the subscriber is connected to.

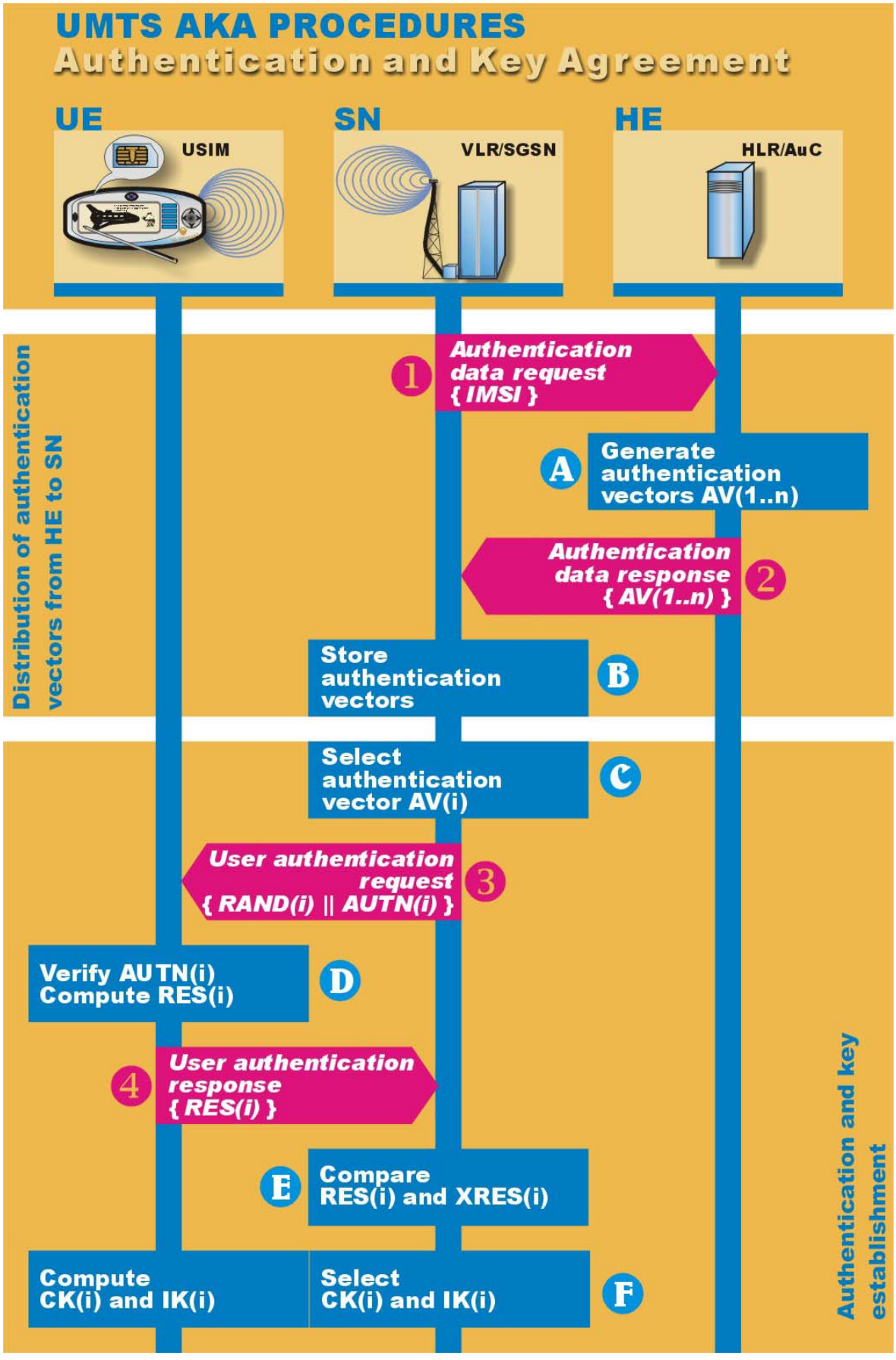

Figure 5 Sequence diagram of AKA.

1 VLR/SGSN in charge of the mobile sends an 'Authentication data request (IMSI)' to the subscriber's Home Location Register.

2 HLR answers with an 'Authentication data response (AV_1,AV_2,… AV_n)'.

3 VLR/SGSN sends 'User authentication request (RAND(i)||AUTN(i))' to the USIM, through the RNC, Node B and Terminal.

4 USIM sends an 'User authentication response (RES(i))' back to the VLR/SGSN.

A. The AuC retrieves/generates the AVs.

B. VLR/SGSN stores AVs in its database.

C. VLR/SGSN selects one of AVs received (in 2).

D. USIM verify AUTN and computes the User Response (RES).

E. VLR/SGSN compares the RES and XRES to authenticate the user.

F. USIM generates the cipher and integrity keys, CK and IK, and VLR/SGSN retrieves the CK and IK of the current AV.

5.1.1 AKA procedure in the AuC

The home location register receives the 'Authentication data request (IMSI)' message from the VLR/SGSN and locates the AuC that the subscriber data is stored on and asks this centre for AVs.

If the AuC has stored AVs for the subscriber, it replies with one or more of these, or else it generates them first. Multiple AVs (up to five) will typically be returned at a time. This is to reduce the number of queries to the AuC and minimize the network traffic. But if the current load on the AuC is high, it might return just one. More AVs will then be generated when the processing load diminish and will be ready for future queries.

5.1.2 AKA procedure in the USIM

Upon receipt of the 'User authentication request (RAND(i)||AUTN(i))' from the VLR/SGSN, the USIM verifies the Authentication Token to authenticate the network. This is done by showing knowledge of a secret key indirectly. The authentication of the network is the first part of the two-way authentication in the one-pass message flow. The USIM then generates the response to be sent back to the VLR/SGSN.

5.1.3 AKA procedure in the VLR/SGSN

The VLR/SGSN is in charge of the Authentication and Key Agreement. It starts the procedures by sending the 'Authentication data request' to the HLR. When it receives the AV(s) it stores them and chooses one, typically the first (AV(1)) and sends two of the parameters, RAND and AUTN of that AV to the USIM.

When it receives the result, RES, from the USIM it compares this with the stored X-RES for that same AV. If they are equal, the network has authenticated the subscriber. The second half of the two-way authentication has completed.

The VLR/SGSN then gets the cipher and integrity keys from the same AV, AV(i) and sends these to the RNC currently holding the subscriber. These are then used for ciphering the communication and integrity checking of the messages.

5.1.4 USIM rejects challenge

If the authentication of the network fails, the USIM will reject it. This is an indication that the challenge received does not originate in the subscriber's Home Environment.

The USIM receives the RAND||AUTN pair, open the AUTN and compares the X-MAC delivered with the MAC itself generates. If these does not compare, the authorization is rejected. It shows that the secret key K is not the same in the two domains, so the message does not originate in the subscriber's home environment.

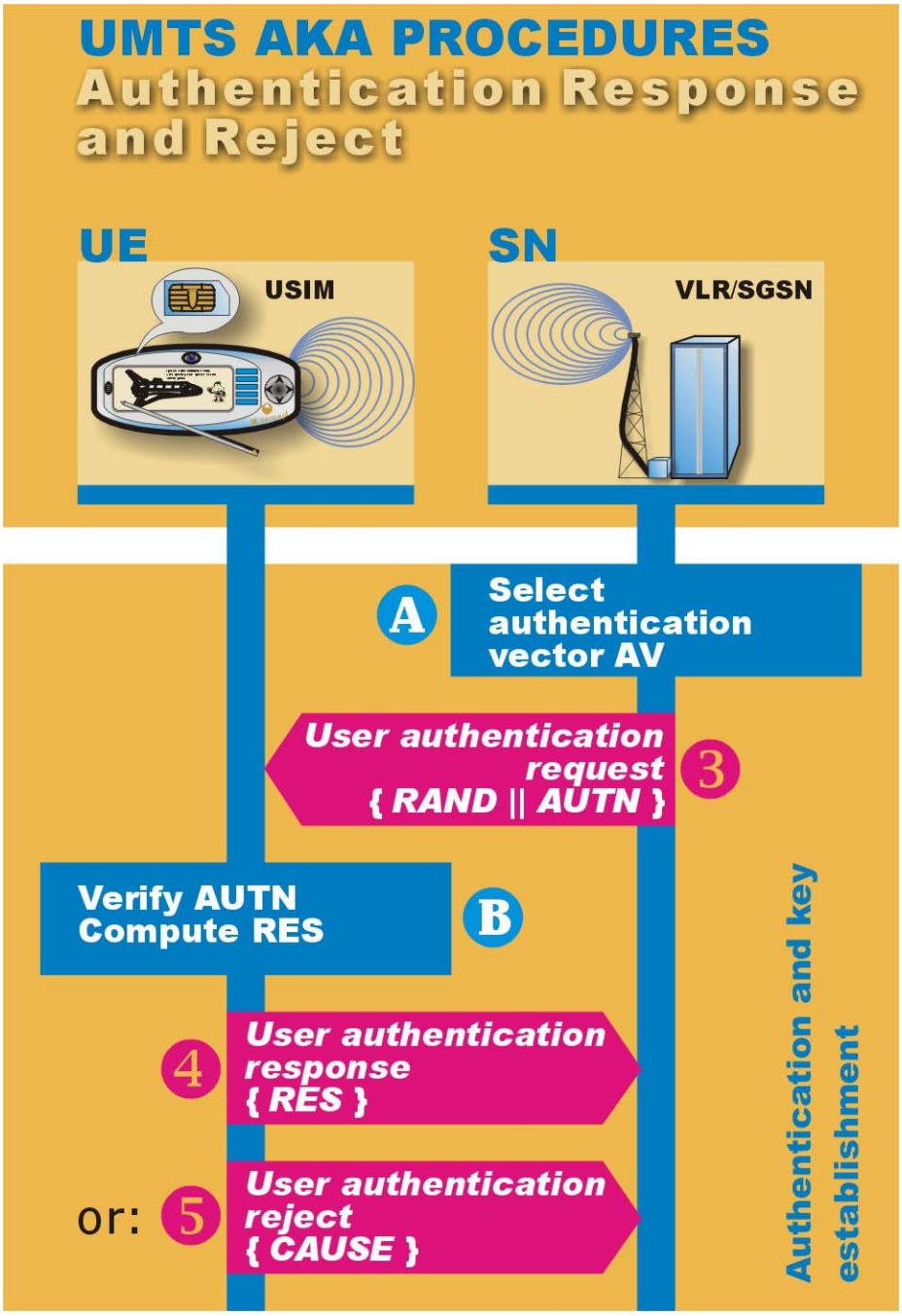

Figure 6 Authentication response and reject procedure.

The USIM checks the message authentication code found within the authentication token. If the delivered X-MAC does not compare with the generated MAC, it abandons the authentication procedure and sends an 'User authentication reject (cause)' message back to the VLR/SGSN.

This will make the VLR/SGSN send an 'Authentication Failure Report' to the HLR, with the subscriber identity and the failure cause attached. It may also restart the Authentication and Key Agreement procedures towards the user.

5.2 AKA resynchronisation procedure

The resynchronisation procedure takes place whenever the sequence numbers in the USIM and AuC is not within a specified range of each other. The difference between them is discovered in the USIM when it compares the received SQN_{HE} with the stored SQN_{ME}.

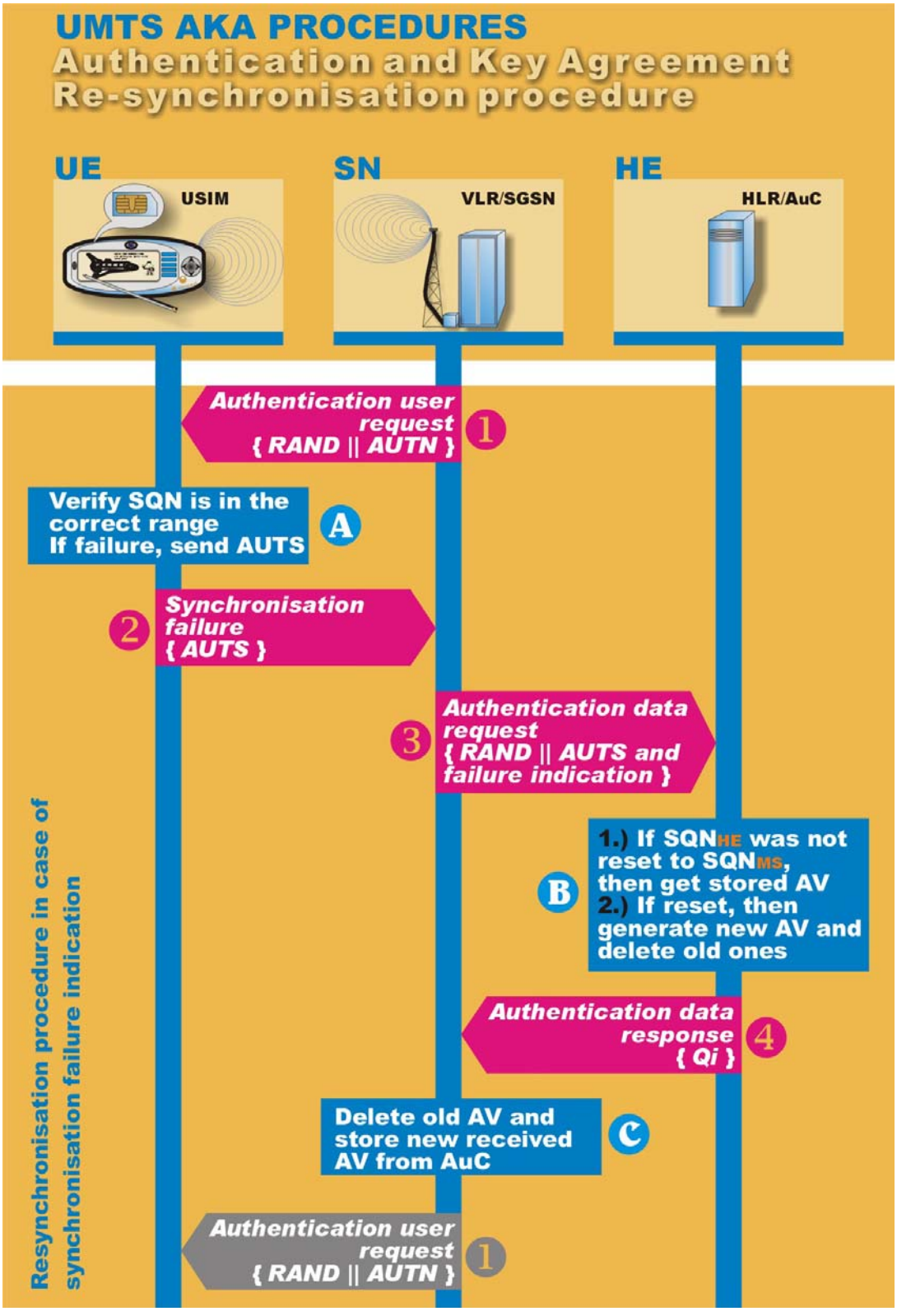

Figure 7 AKA resynchronisation procedure.

1 The VLR/SGSN sends a normal 'User authentication request (RAND(i)||AUTN(i))' to the USIM.

2 When the USIM finds the sequence number of the AuC out of range, it sends a 'Synchronisation failure (AUTS)' message back to the VLR/SGSN.

3 The VLR/SGSN node keeps track of the AVs sent to the USIM and when it receives the message with the re-synchronisation token, AUTS, it attaches the RAND(i) it sent, and sends an 'Authentication data request (RAND(i)||AUTS)' message to the subscriber's HLR/AuC.

4 The AuC sends an 'Authentication Data Response(AV)' back to the VLR/SGSN. AVs are also called Quintets. To indicate that there is a newly made AV sent back, the parameter Q_i is used.

A. USIM verifies that SQN_{HE} is within the range of SQN_{MS}. If the SQN_{HE} is out of range, the USIM generates the Re-synchronisation Token (AUTS).

B. When HE receives the AUTS, it compares the two sequence numbers. If it finds that the next generated AV will be accepted by the USIM, it retrieves/generates the AV with this sequence number.

Otherwise, the AuC opens the AUTS to authenticate the user and to reset the SQN_{HE} to the value of SQN_{MS}. It then deletes the old AVs and generates new based on the reset SQN value.

C. When the VLR/SGSN receives AVs, in response of an 'Authentication Data Request' with synchronisation failure indication, it is to delete all previously stored AVs.

1 VLR/SGSN continues the AKA procedure to challenge the USIM (See number 3 in Figure 5)

5.2.1 Resynchronisation procedure in the USIM

When the USIM receives the 'User authentication request(RAND(i)||AUTN(i))' message from the VLR/SGSN it starts by checking the authenticity of the message. If it is generated at the home environment it proceeds to check the sequence numbers of the AuC compared to it's own.

If the sequence number is out of range, then the resynchronisation procedure takes place. The USIM generates a re-synchronisation token, AUTS, to be sent back to the VLR/SGSN.

5.2.2 Resynchronisation procedure in the AuC

The AuC receives the 'Authentication data request (RAND(i), AUTS, synchronisation failure))' message from the VLR/SGSN. Then it compares the two sequence numbers. It may find that the next generated AV will be accepted, and will then send this back to the VLR/SGSN.

If none of the stored AVs will be within range accepted by the USIM, the AuC performs integrity check of the message. This is to make sure that it's the actual USIM who wishes to perform the full resynchronisation procedure. If the authentication completes successfully, the sequence number of the AuC, SQN_{HE}, is set to the value of the SQN_{MS}.

When the sequence number of the AuC gets reset, it has to generate a new set of AVs. Real-time generation of multiple AVs may, as mentioned earlier, generate too much workload for the AuC and therefore it may just return one AV in the first response.

5.2.3 Resynchronisation procedure in the VLR/SGSN

The VLR/SGSN finds the appropriate random challenge (RAND) from its memory when it receives the 'Synchronisation failure' and adds this to the message before sending it to the subscriber's Home Location Register.

When it receives the AVs from the AuC, will delete all other old AVs for that subscriber. This is to reduce the problem of performing another AKA procedure that will surely lead to another resynchronisation failure.

After receiving new AVs, the VLR/SGSN can continue the Authentication and Key Agreement procedure towards the USIM.

5.3 When to perform AKA

Authentication and Key Agreement is performed when:
- Registration of a user in a Serving Network
- After a service request
- Location Update Request
- Attach Request
- Detach request
- Connection re-establishment request

Registration of a subscriber in a serving network typically occurs when the user goes to another country. The coverage area of an operator is nationwide, and roaming between national operators will therefore be limited. The first time the subscriber then connects to the serving network, he gets registered in the Serving Network.

Service Request is the possibility for higher-level protocols/applications to ask for AKA to be performed. E.g. performing AKA to increase security before an online banking transaction.

The terminal updates the HLR regularly with its position in Location Update Requests.

Attach request and detach request are procedures to connect and disconnect the subscriber to the network.

Connection re-establishment request is performed when the maximum number of local authentications has been conducted.

5.4 Re-use of AVs

Re-use of AVs are rejected by the USIM because of the sequence number checking. This is to prevent a network to perform Authentication and Key Agreement repeatedly using the same AV.

Though sometimes, re-use of AVs are necessary. Like when the VLR/SGSN sends a 'User authentication request' message to the USIM, but never gets a reply (caused by network failure, empty battery etc). When the timeout of waiting for the reply exceeds, it will try to resend the same RAND||AUTN pair to the USIM again. If the USIM actually did get the AV the first time, but the answer never reached the VLR/SGSN, it will see that the sequence number received is out of range. To keep from starting the resynchronisation procedure in these cases, the USIM always starts by comparing the incoming random challenge with the previous random challenge received. If they match, it will only resend the last saved user response. All parameters generated at the USIM should for this reason always be stored.

5.5 Emergency call handling

Even when performing emergency calls the authentication procedures will be performed. But if the authentication fails, either by having no USIM, no roaming agreement or other network failure, the connection will be set up anyway. The call will be disconnected only if the confidentiality and integrity protection applied fails.

6 AKA algorithms

The security features of UMTS are fulfilled with a set of cryptographic functions and algorithms. A total of 10 functions are needed to perform all the necessary features, f0-f5, f1*, f5*, f8 and f9.

f0 is the random challenge generating functions, the next seven are key generating functions, so they are all operator specific. The keys used for authentication are only generated in the USIM and the AuC, the two domains that the same operator is always in charge of.

Function f8 and f9 are used in USIM and RNC, and since these two domains may be of different operators, they cannot be operator specific. The functions use the pre-shared secret key (K) indirectly. This is to keep from distributing K in the network, and keep it safe in the USIM and AuC.

Table 1 AKA functions with their outputs.

Function	Description	Output
f0	The random challenge generating function	RAND
f1	The network authentication function	MAC-A/XMAC-A
f1*	The re-synchronisation message authentication function	MAC-S/XMAC-S
f2	The user authentication function	RES/XRES
f3	The cipher key derivation function	CK
f4	The integrity key derivation function	IK
f5	The anonymity key derivation function	AK
f5*	The anonymity key derivation function for the re-synchronisation message function	AK
f8	The confidentiality key stream generating function	<Keystream block>
f9	The integrity stamp generating function	MAC-I/XMAC-I

6.1 Requirements for cryptographic functions and algorithms

The cryptographic functions and algorithms must meet stringent requirements. The functions should be designed with a view to its continued use for a period of at least 20 years. Successful attacks with a workload significantly less than exhaustive key search through the effective key space should be impossible.

User Equipment that holds these functions should be free from restrictions on export and use. Network equipment, like RNCs and AuCs may expect to meet such restrictions. The export of these nodes should comply with the Wassenaar Agreement. This way each operator can set up equipment and algorithms according to local laws and licenses, and the users can roam with their own equipment without having to change it whenever entering a new operator/country.

Without knowledge of input keys, the functions should be indistinguishable from independent random functions of their inputs. Changing of one parameter at a time should not reveal any information about either the secret key K or the operator variant configuration field, OP.

6.1.1 Implementation of functions

The functions f1-f5, f1* and f5* shall be designed so that they can be implemented on an IC card equipped with a 8-bit microprocessor running at 3.25MHz with 8kbyte ROM and 300byte RAM and produce AK, XMAC-A, RES, CK and IK in less than 500ms execution time.

6.2 Key generating functions

The functions f1-f5* are called key generating functions and are used in the initial Authentication and Key Agreement procedures.

6.2.1 Normal functions in the AuC

When generating a new AV the AuC (AuC) reads the stored value of the sequence number, SQN_{HE} and then generates a new SQN and a random challenge RAND. Together with the stored AV and Key Management Field (AMF) and the pre-shared secret key (K), these four input parameters are ready to be used.

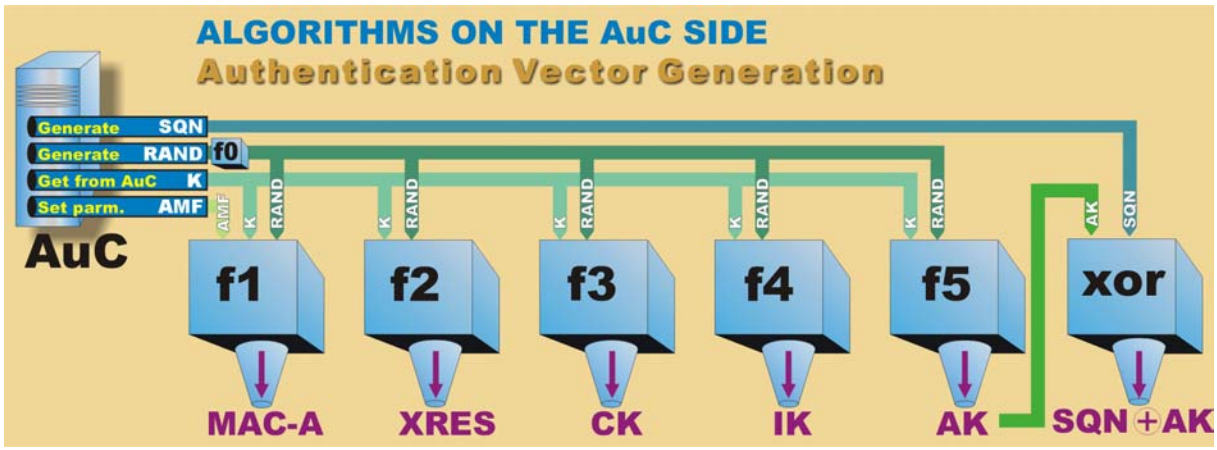

Figure 8 AV generation in the AuC.

The functions uses these inputs and generates the values for the message authentication code, MAC-A, the expected result, X-RES, the Cipher Key (CK), the Integrity Key (IK) and the Anonymity Key (AK). With the SQN⊕AK, AMF and MAC, the Authentication Token, AUTN can be made. AUTN are the three parameters concatenated.

6.2.2 Normal functions in the USIM

To generate the output keys in the USIM it has only one of the four parameters that the AuC have, the pre-shared secret key (K). The rest of the parameters it has to receive from the AuC.

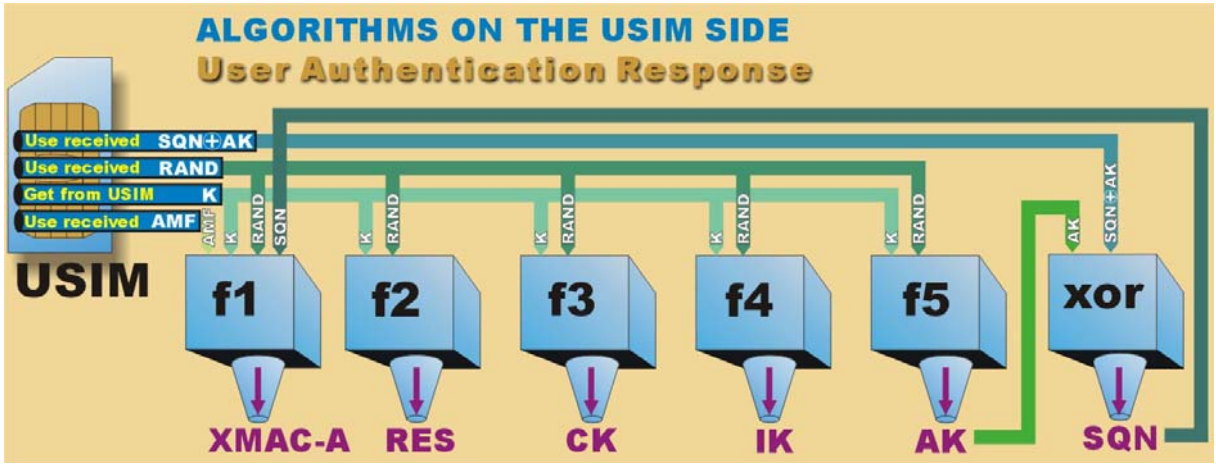

Figure 9 RES generation in the USIM.

When the USIM receives the (RAND||AUTN) pair it starts by generating the Anonymity Key (AK) by applying function f5 on the received RAND. By XOR-ing the AK with the (SQN⊕AK) from the Authentication Token, the sequence number of the AuC is revealed (SQN_{HE}).

The secret key K is then used with the received AMF, SQN and RAND to generate the Expected Message Authentication Code (XMAC-A). This is then compared with the MAC-A. If the X-MAC and MAC matches, the USIM have authenticated that the message (RAND||AUTN pair) is originated in its Home Environment (and thereby connected to a Serving Network that is trusted by the HE) and the key generating functions can continue.

If the X-MAC and MAC are different from one another, a 'user authentication reject' is to be sent back to the VLR/SGSN with indication of the cause and the user then abandons the procedure.

With a successful network authentication, the USIM verifies if the sequence number received is in within the correct range (defined by each network operator). If the sequence number is not within the correct range a 'synchronisation failure' message is to be sent to VLR/SGSN (see 6.2.3).

With a sequence number within the correct range, the USIM continues to generate the RES by function f2 with the input parameters K and RAND.

6.2.3 Resynchronisation functions in the USIM

When the USIM finds the received sequence number out of range, the normal key generating function abandons and the USIM starts to generate a re-synchronisation token, AUTS.

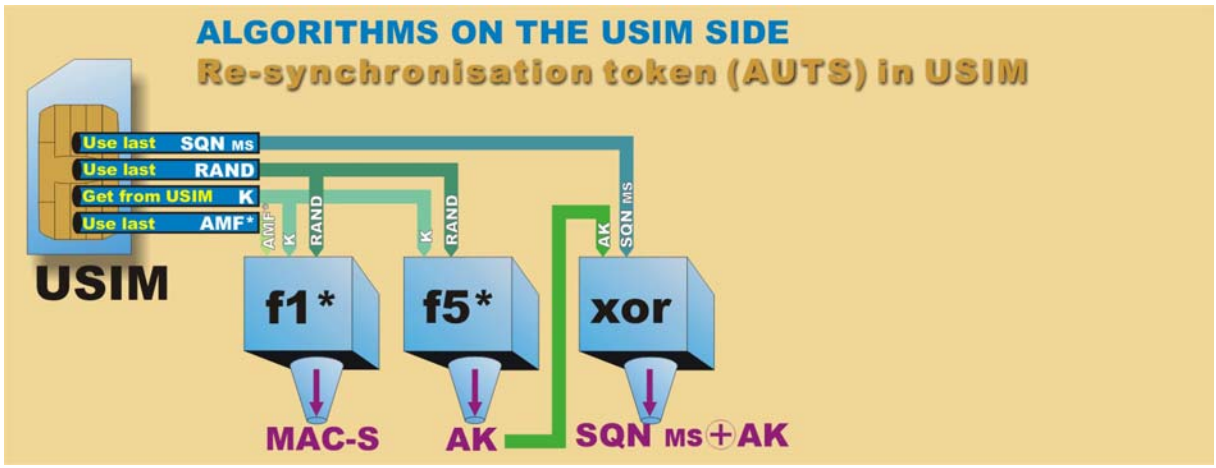

Figure 10 AUTS generation in the USIM.

The authentication and key management field, AMF, is set to all zeros to keep from being transmitted in clear in the re-synch message.

The Resynchronisation Message Code (MAC-S) is then generated in function f1* with the sequence number stored in the USIM, SQN_{MS}, the received random challenge, RAND, the all zero set AMF and the pre-shared secret key (K) as inputs. The function f5* then generates the special resynchronisation anonymity key, AK to conceal the sequence number.

The MAC-S and the $SQN_{MS} \oplus AK$ are the then concatenated into AUTS. A 'synchronisation failure' message with the AUTS as parameter is then sent back to the VLR/SGSN.

The special functions f1* and f5* are only used for the re-synchronisation procedures. These functions are made in such a way that their values will not reveal anything of the other functions.

6.2.4 Resynchronisation functions in the AuC

The AuC receives the RAND||AUTS pair from the VLR/SGSN.

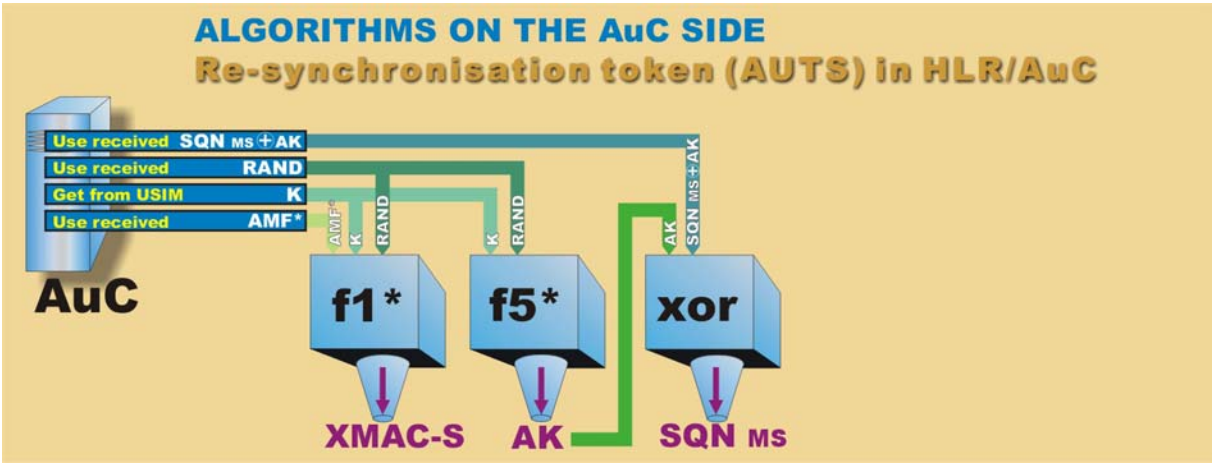

Figure 11 Resynchronisation procedure in the AuC

The function f1* is used with K and the received parameters RAND and AMF to generate the Expected Resynchronisation Authentication Code (XMAC-S). This is compared with the received MAC-S and continues with the procedure if they match.

The function f5* is used with the received RAND to retrieve the Anonymity Key, that again will give the sequence number of the USIM (SQN_{MS}).

Then the AuC compares the two sequence numbers. It may find that the next generated AV will be accepted, and will then send this back to the VLR/SGSN. If none of the stored AVs will be within range accepted by the USIM, the VLR/SGSN generates the XMAC-S and compares it with the MAC-S received in the authentication token, AUTS. This is to authenticate the subscriber, and if it is successful, the sequence number of the AuC, SQN_{HE}, is set to the value of the SQN_{MS}.

When the sequence number of the AuC (SQN_{HE}) is reset, it has to generate a new set of AVs. Real-time generation of multiple AVs may, as mentioned earlier, generate too much workload for the AuC and therefore it may return just one AV in the first response.

6.2.5 Order of key generation

The order of key generation may not be implemented as described above. The description is of the logical order but the implementation may differ, if it seems to be more efficient. In any case, the keys have to be ready in the order mentioned above.

6.3 Authentication parameters

The following parameters are used in the Authentication and Key Agreement procedure:

- AV
- AUTN
- RES and XRES
- MAC-A and XMAC-A
- AUTS
- MAC-S and XMAC-S

6.3.1 AV

AVs are generated at the AuC and are put together and sent to the Serving Network where it is used for authentication. When the authentication is performed, the cipher and integrity keys of the AV are copied to the RNC.

Table 2 Parameters of the AV.

Parameter	Description
RAND	The random challenge to be sent to the USIM
XRES	The expected result from the USIM
AUTN	Authentication token that authenticates the AuC towards the USIM.
CK	Cipher key for confidentiality
IK	Integrity key for integrity checking

6.3.2 AUTN

The Authentication Token (AUTN) is generated at the AuC and sent with the Random Challenge (RAND), from the VLR/SGSN to the USIM. The AUTN is made up by the SQN_{HE}, the AMF and the MAC-A.

$AUTN = SQN_{HE} \oplus AK \,||\, AMF \,||\, MAC\text{-}A$

6.3.3 RES and XRES

The user response RES, is used by the network to authenticate the subscriber. The XRES is generated first in the AuC and sent to the VLR/SGSN in the AV. Then the USIM generates the RES and sends it to the VLR/SGSN, where the two are compared. And if they match, the user is authenticated to the network.

$RES = f2(K, RAND)$

6.3.4 MAC-A and XMAC-A

The Network Authentication Code (MAC-A) and Expected Network Authentication code (XMAC-A) are used in authentication and key agreement for the USIM to authenticate the network. The MAC-A is generated at the AuC and the XMAC-A at the USIM. The USIM receives the MAC-A and compares it with the locally generated XMAC-A. If they match, the USIM has successfully authenticated that the network is operating on behalf of (trusted by) the subscriber's Home Environment.

$MAC\text{-}A = f1(AMF, K, RAND, SQN)$

6.3.5 AUTS

The Re-synchronisation Token is generated at the USIM when the sequence number of the Home Environment is out of range of its own sequence number. The sequence number of the USIM is then sent in the AUTS to the AuC to continue the resynchronisation procedure.

$AUTS = SQN_{MS} \oplus AK \,||\, MAC\text{-}S$

6.3.6 MAC-S and XMAC-S

Resynchronisation Authentication Code (MAC-S) and expected XMAC-S is used to authenticate the USIM before resetting the sequence number of the AuC. When the USIM finds a synchronisation failure, it generates the MAC-S and sends this to the AuC. It generates its own XMAC-S and compares these. If they match, the synchronisation failure message is authenticated and the sequence number of AuC will be reset to the sequence number of the USIM.

$MAC\text{-}S = f1^*(AMF, K, RAND)$

6.3.7 Size of authentication parameters

Table 3 Bit size of authentication parameters.

Parameter	Definition	Bit size
K	Pre-shared secret key	128
RAND	Random challenge	128
SQN	Sequence number	48
AK	Anonymity Key	48
AMF	Authentication Management Field	16
MAC	Message Authentication Code	64
CK	Cipher Key	128
IK	Integrity Key	128
RES	Response	32-128
X-RES	Expected Response	32-128
AUTN	Authentication Token	128 (16+64+48)
AUTS	Authentication re-Synchronisation Token	96-128
MAC-I	Message authentication code for data integrity	32

6.4 Integrity function f9

Most control signalling information elements that are sent between the User Equipment (UE) and the network are considered sensitive and must be integrity protected. On messages transmitted between the UE and the RNC, a message integrity function (f9) shall be applied on the signalling information. User data are on the other hand not integrity protected and it's up to higher-level protocols to add this if needed. Integrity protection is required, not optional, in UMTS for signalling messages.

The function f9 is used in a similar way as the AUTN and the AUTS. It adds a 'stamp' to messages to ensure that the message is generated at the claimed identity, either the USIM or the Serving Network, on behalf of the HE. It also makes sure that the message has not been tampered with.

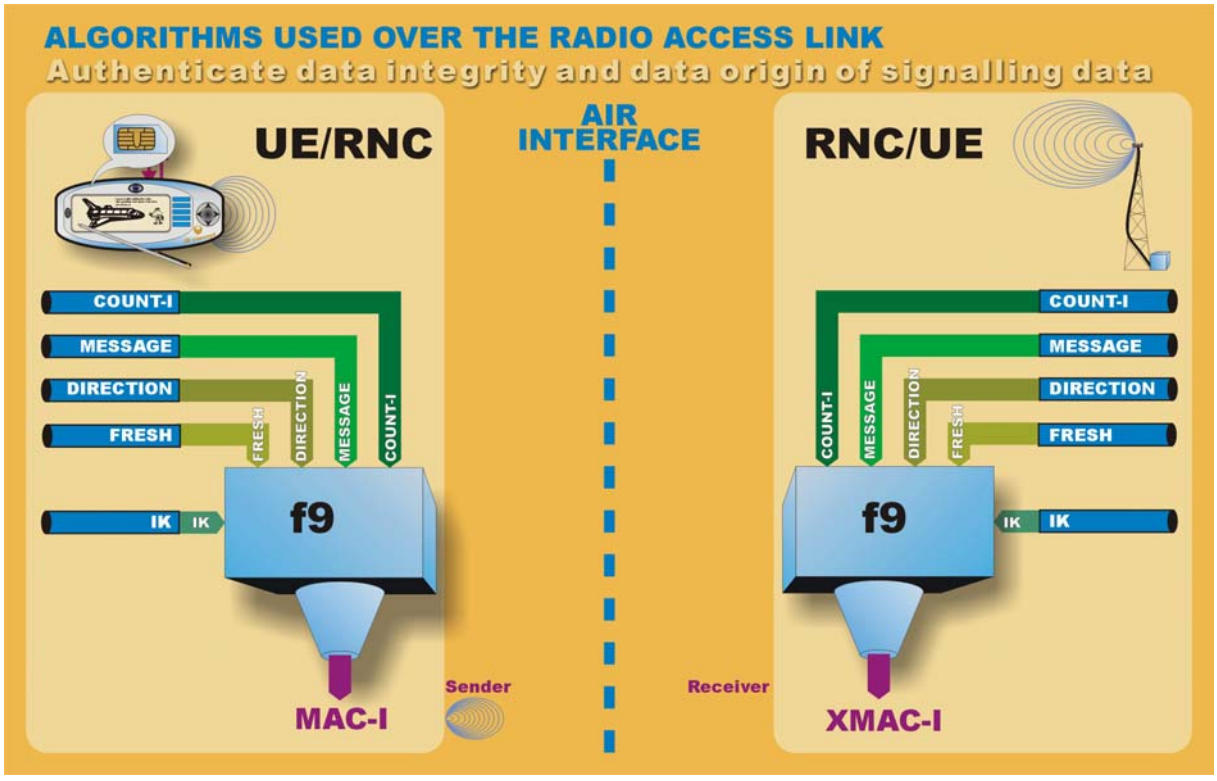

Figure 12 Integrity function f9.

6.4.1 Input parameters to the integrity algorithm

Table 4 Input parameters to function f9.

Parameter	Description	Bit size
COUNT-I	The integrity sequence number	32
IK	Integrity key	128
FRESH	The network-side nonce	32
DIRECTION	Either 0 (UE➠RNC) or 1 (RNC➠UE)	1
MESSAGE	The signalling message itself with the radio bearer identity	

The counter (COUNT-I) is incremented by each integrity-protected message. There are separate counters for uplink and downlink. This, together with the DIRECTION identifier, assures that the input parameters never stay the same within a connection, thus preventing replay attacks.

The Integrity Key (IK) is generated in both the AuC and USIM. The VLR/SGSN receives the IK in the AV from the AuC, and sends it to the RNC after authenticating the USIM. When handovers occur, the Integrity Key is transmitted within the network from the current RNC to the new RNC. The key itself is not changed at handovers.

The network-side nonce FRESH is used to protect against replay attacks. One FRESH value is assigned to each user and the RNC generates this value at connection set-up. It is then sent to the user with a 'security mode command'. The lifetime of the FRESH value is one connection and new FRESH will be generated at the next connection. Also at handovers, the FRESH will be reset to a new value.

The direction identifier (DIRECTION) is used to distinguish between messages being sent and messages being received. This it to prevent the function from using the same input parameters for messages being sent and received. The direction identifier is 1 bit, with value '0' for messages from the USIM to the RNC, uplink, and '1' for messages from the RNC to the USIM, downlink.

The message itself is an important input to the function. Only by doing this, the integrity of the message can be protected. If anyone changes the message between the sender and receiver, the receiver will not get an XMAC-I matching the MAC-I received. This will make the receiver just reject the message.

6.4.2 MAC-I and XMAC-I

Message Authentication Code for Data Integrity (MAC-I) and the expected XMAC-I are used after the authentication and key agreement procedures are finished. The MAC-I is generated at the sender side (either USIM or RNC) and compared with the XMAC-I at the receiver side (respectively RNC or USIM). The sender generates the MAC-I with the message itself as an input, and the receiver uses the attached message to its own function and generates the XMAC-I. If they match, the message proves to be unaltered and it's origin authenticated. If it fails, the message it rejected.

MAC-I = f9(COUNT-I, Message, DIRECTION, FRESH, IK)

6.4.3 UIA identification

Since the UMTS Integrity Algorithm (UIA) will be both in the USIM and the RNC, they may be in different operator's domains. Because of this, the different nodes may support different algorithms. To identify the different algorithms used, every UIA will have each own 4-bit identifier.

The USIM will provide the RNC with information on which UIAs it supports and it is then up to the RNC to decide (by the operator's preference) which UIA will be used consequently.

6.4.4 Messages that are not integrity protection

Some messages does not include integrity protection, these messages are:

- HANDOVER TO UTRAN COMPLETE
- PAGING TYPE 1

- PUSCH CAPACITY REQUEST
- PHYSICAL SHARED CHANNEL ALLOCATION
- RRC CONNECTION REQUEST
- RRC CONNECTION SETUP
- RRC CONNECTION SETUP COMPLETE
- RRC CONNECTION REJECT
- RRC CONNECTION RELEASE (CCCH only)
- SYSTEM INFORMATION (BROADCAST INFORMATION)
- SYSTEM INFORMATION CHANGE INDICATION
- TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

6.5 Confidentiality function f8

User data and some signalling information elements are considered sensitive and must be confidentiality protected. To ensure identity confidentiality, the temporary user identity (P-)TMSI must be transferred in a protected mode at allocation time and at other times when the signalling procedures permits it. The need for protected mode of transmission is fulfilled by a confidentiality function that is applied on dedicated radio access link channels between the UE and the RNC.

The cipher function f8 is a keystream cipher that generates a keystream block. This is XOR-ed with the user plaintext block and then sent over the air. The cipher keystream that are generated are unique for every block. It does not generate one key per session that all the blocks of size LENGTH are XORed with, but a new key for all the blocks. Because of this both sender and receiver have to be synchronised with the same counter at all times, or else the decryption will fail.

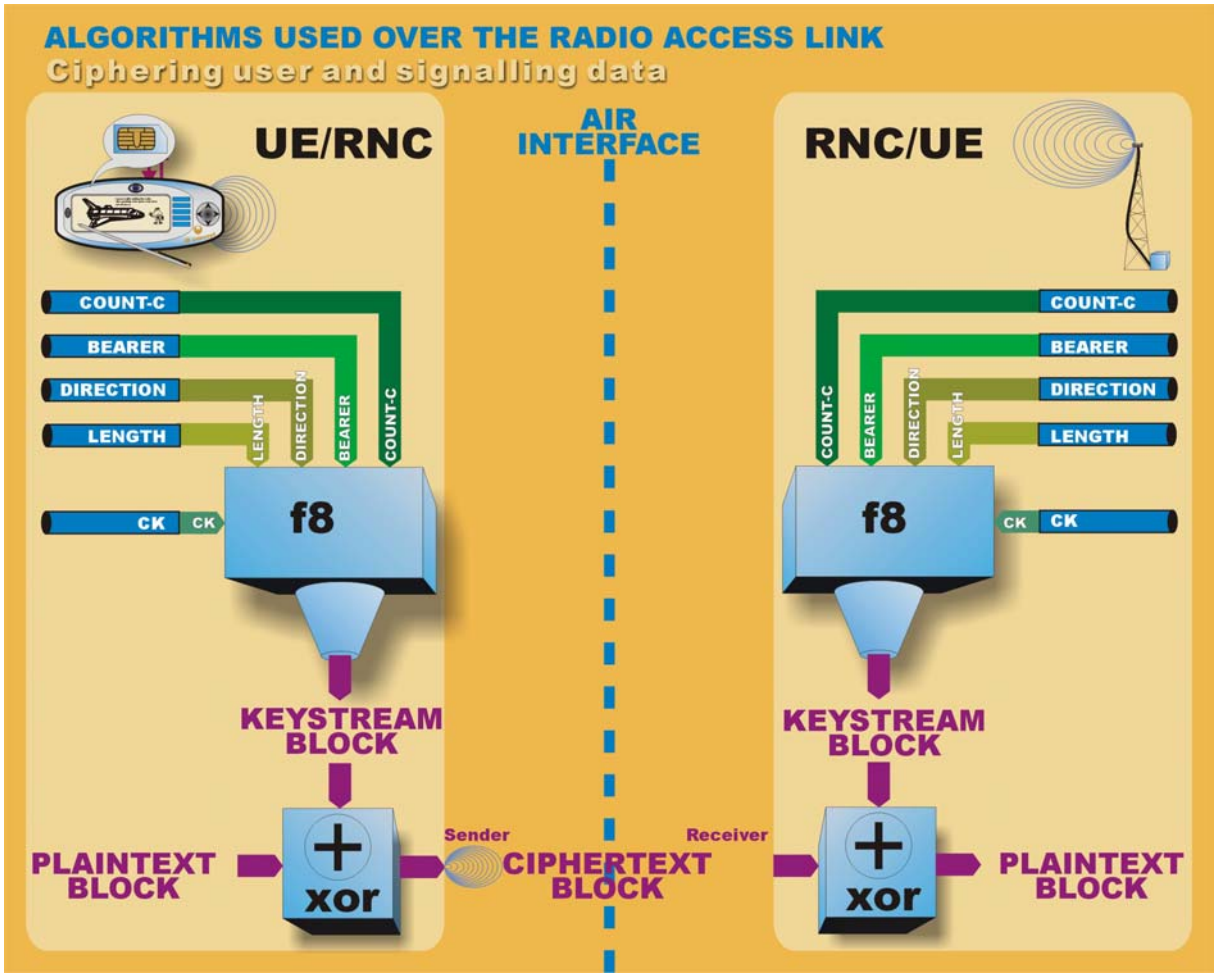

Figure 13 Confidentiality function f8.

6.5.1 Input parameters to the cipher algorithm

Table 5 Input parameters to function f8

Parameter	Description	Bit size
COUNT-C	The ciphering sequence number	32
CK	Cipher key	128
BEARER	The radio bearer identifier	5
DIRECTION	Either 0 (UE -> RNC) or 1 (RNC->UE)	1
LENGTH	The actual length of the keystream block	16

The counter (COUNT-C) is incremented by each confidentiality-protected message sent or received. There are separate counters for uplink and downlink. This, together with the DIRECTION identifier, assures that the input parameters never stay the same within a connection.

There may be one Cipher Key (CK) for circuit switched connections (CK_{CS}), established between the circuit switched service domain and the user; and another cipher key for packet switched connections (CK_{PS}) established between the packet switched service domain and the user.

The cipher key is generated in the AuC and sent to the VLR/SGSN as a part of the AV. When the authentication of the subscriber has been completed successfully, the key is to be sent from the VLR/SGSN to the RNC. The USIM generates it's own CK during the authentication procedures.

When performing handover, the CK is transmitted in the network from the current RNC to the new RNC, to enable the communication to proceed. The CK remains unchanged at handovers.

The bearer identifier (BEARER) is used to distinguish between different logical radio bearers associated with the same user on the same physical link. This is done to avoid having the same input parameters, thus same keystream for different radio bearers.

The direction identifier (DIRECTION) is used to distinguish between messages being sent and messages being received to prevent the function from using the same input parameters. The direction identifier is 1 bit, with value '0' for messages from the USIM to the RNC, uplink, and '1' for messages from the RNC to the USIM, downlink.

The LENGTH parameter is used to give the length of the output keystream block. The parameter itself will not affect the bits in the keystream, just the number of bits in it.

6.5.2 UEA identification

As with the integrity function, the cipher function is also possibly managed by two different operators at a time. This makes the UMTS Encryption Algorithm (UEA) identification important. The same encryption algorithms have to be used in both the USIM and RNC. The USIM lets the RNC know which encryption algorithms, if any, are supported. The RNC then chooses, by network preference and regulations, what encryption algorithm to use.

While integrity protection is required, confidentiality protection is just an option, however the user should be informed whether encryption is enabled or not.

6.6 Key lifetime

A call set-up does not automatically trigger Authentication and Key Agreement, and to ensure that old keys are not used for an unlimited (as long as the terminal is 'on') period of time the USIM keeps counters of how long the keys have been used for. The maximum limit for use of same keys are defined by the operator, and whenever the USIM finds the keys being used for as long as allowed, it will trigger the VLR/SGSN to use a new AV.

6.7 Milenage

By making this function set, ETSI reduces the implementing cost for the operators. They may choose to implement only function f9 of the Milenage set, and make their own implementations of the other functions, but this will surely be very expensive and probably less secure. The Milenage function set has been tested extensively and found robust.

6.8 KASUMI algorithms

The KASUMI algorithms are the core algorithms used in functions f8 and f9. Kasumi is based on the block cipher 'Misty', presented by Mr. Matsui in 1997. The rights Misty is held by Mitsubishi Electric corp., which let ETSI use these algorithms for UMTS. The Misty algorithms were adjusted in some ways to better fit the needs of UMTS and then called KASUMI. The name Kasumi is Japanese for misty.

7 Illustrator

7.1 Illustrator functionality explanation

The UMTS AKA Illustrator

The main purpose of the 'UMTS AKA Illustrator' is to show how authentication and security procedures are done in UMTS. We figured out that an animation is the best way to accomplish this. So, by using Flash 5 technology we were able to create small movie clips of each relevant procedure.

7.1.1 Main menu system:

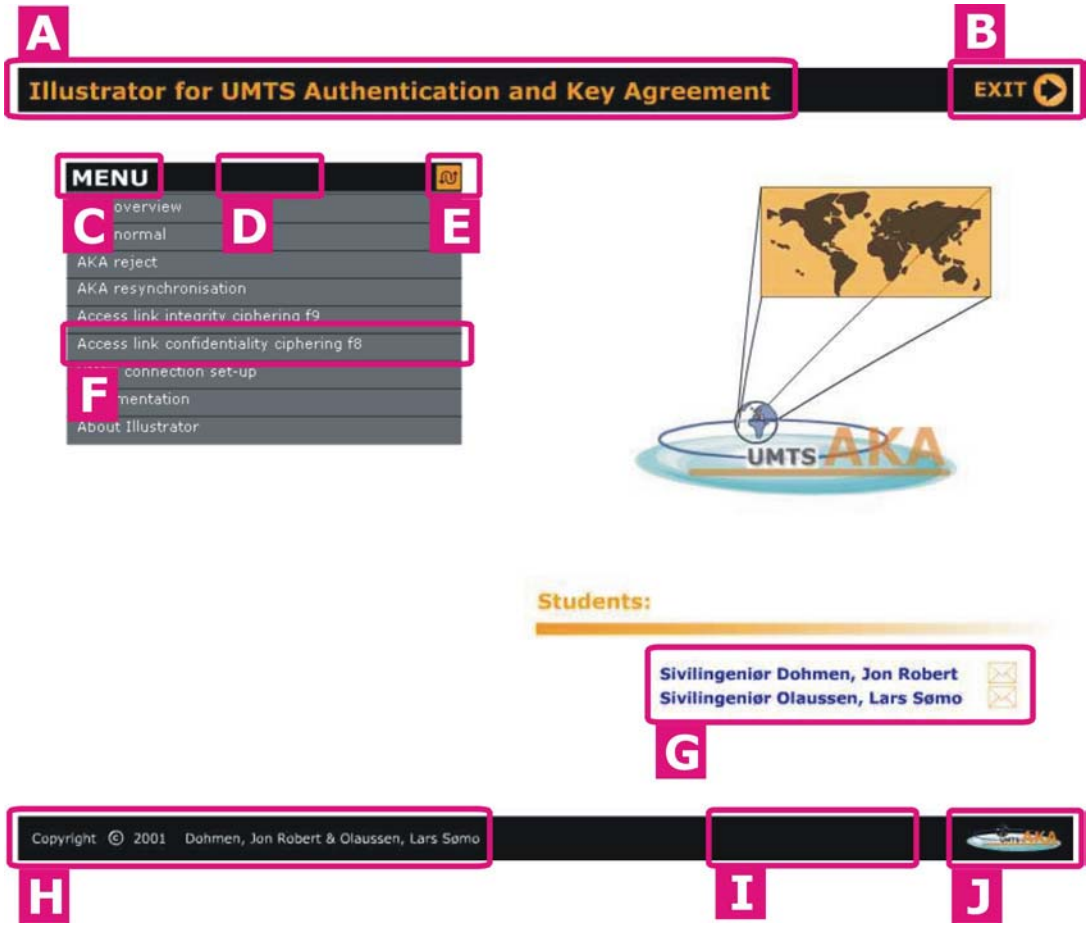

Figure 14 Main menu of the illustrator

The Figure 14 shows a snapshot image of the user interface for the main menu system. Each item on the image is marked with a flag and a letter. Each flag have the following meaning:

A. This heading represents the title of the menu. This is the main menu system, and it is called 'Illustrator for UMTS Authentication and Key Agreement', here after referred to as 'Illustrator'. However, there is one more sub-menu called 'Documents Menu'.

B. This is representing an exit-button that escapes the program totally and leaves the browser or Flash projector empty. In the sub-menu 'Documents Menu' the button is located at the same place, but returns the user back to the 'Illustrator for UMTS Authentication and Key Agreement'. In any movie clip the button is also located at the

same place, but will bring the user back to the main menu.

C. This menu contains an item for all animated movie clips available in the Illustrator.

D. The menu is not statically placed on the background, but drag-able by pushing the mid part of the menu, in a drag-and-drop manner. (There is no real need for this function at this stage, but was intended to be used in a different way under the development phase of the Illustrator. Perhaps in a further developed menu system this feature could be used).

E. The menu can be collapsed to become one line high, thus taking up lot less space, e.g. drop-down menu. (There is no real need for this function at this stage, but was intended to be used in a different way under the development phase of the Illustrator. Perhaps in a further developed menu system this feature could be used).

F. Each line in the drop down menu represents selectable menu items. In the menu we can find the following options:

AKA overview:
- This movie clip is an overview of the AKA procedures and does not contain any explanation of the functions taking place at AuC and USIM side

AKA normal:
- This movie clip shows a 'normal' authentication procedure inclusive all calculation of functions at both AuC and USIM side.

AKA reject:
- This move clip shows a user being rejected due to wrong integrity code.

AKA resynchronisation:
- This movie clip shows a user with correct integrity, but wrong sequence number that is initiating resynchronisation procedure.

Access link integrity ciphering f9:
- This movie clip is basically showing how a message authentication code is integrity protecting a message over the radio access link.

Access link confidentiality ciphering f8:
- This movie clip is showing how a stream of user data is kept confidential by mixing it with a unique keystream over the radio access link.

UMTS connection set-up:
- This movie clip is showing how a connection is set-up sequence diagram. The diagram is showing when AKA is performed and also when to initiate integrity and confidentiality ciphering over the radio access link.

Documentation:
- This option leads to a sub-menu, 'Documents Menu', that contains relevant documents such as this graduate thesis and full screen size static JPEG-images.

About Illustrator:
- This page contains some copyright information and some system info.

The menu item 'Documents' has a sub-menu, which contains illustrations using JPEG-images in a static manner. These illustrations are showing all the procedures discussed in the thesis. In this sub-menu we can find the following options:
- Thesis in Word2000-format (*.doc)
- Thesis in Acrobat-format (*.pdf)
- Thesis in Hypertext-format (*.htm)
- UMTS overview
- AKA overview
- Connection set-up overview
- CS and PS domain overview

- Generating functions for normal AKA
- Generating functions for resynch AKA
- Integrity ciphering f9
- Confidentiality ciphering f8
- Sequence diagram AKA normal
- Sequence diagram AKA resynch
- Sequence diagram UMTS IMSI
- Sequence diagram UMTS IMSI/TMSI
- UMTS security architecture 1
- UMTS security architecture 2

G. These are the names of the creators of this Illustrator. The Illustrator should not be used without permission of the creators and owners. There is an e-mail address attached to each mail symbol that can be used.

H. This product is under copyright by Dohmen, Jon Robert and Olaussen, Lars Sømo. Any use should be agreed upon before the Illustrator is being used.

I. This area contains a clock and date label showing: day, month and year.

J. To distinguish this Illustrator from other products this logo is especially made for this project.

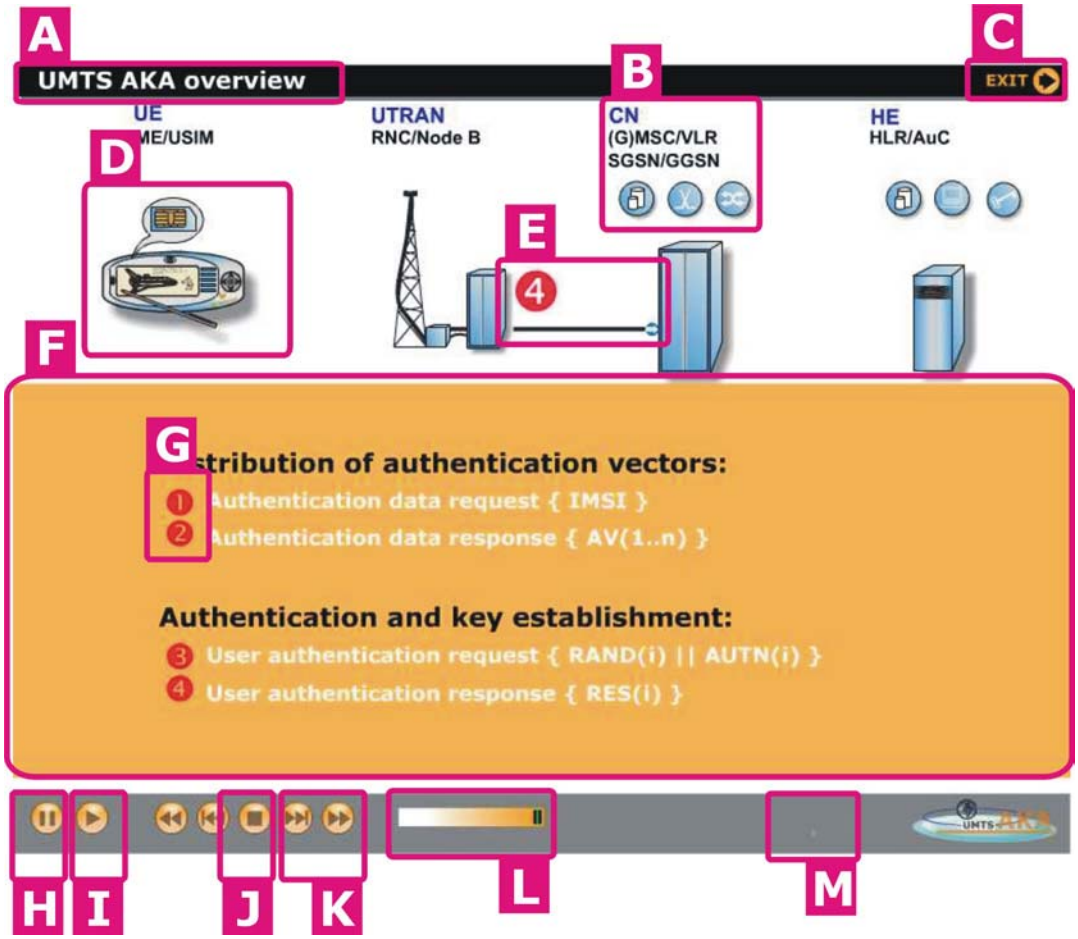

Figure 15 Typical user interface of movie clip.

7.1.2 General example of movie clip

A. This line shows the name of the current movie clip.

B. These labels indicate the current UMTS node/object in action. Some symbols have been added to increase the understanding of the PS /CS domain and Home Environment (HE), e.g. switching symbol, routing symbol, database symbol, AuC key storage symbol etc.

C. In any movie clip that is loaded by the main menu this exit-button will bring the user back to the main menu. The term 'exit-button' could seem a tad misleading, but it is labelled 'EXIT' for a reason. Each movie clip could be played as a stand-alone application and will in that case exit the program.

D. Each UMTS element is represented with a graphically symbol. The UE is illustrated with a future terminal concept drawing containing a UICC card (with USIM program). UTRAN is combined of two elements; Radio Network Controller (RNC) and Node B (base station radio tower) to simplify the UMTS complexity. The CN (CN) actually consists of many elements, but indicated to be one unit here, since AKA is alike for the to CS and PS domains. The Home Environment (HE) consists of HLR and AuC elements.

E. Whenever a signal is transferred between to nodes in the UMTS system this is represented by an animation showing whether the signal is airborne (radio waves) or by wire/link connection (bit stream).

F. This is the main action area for the Illustrator. In this area all information will be laid out, whether it is plain text or actions taking place within each node. See also G. below.

G. Each item (e.g. numbered text elements) will correspond with transmissions between each node, see E.) above. Numbers in this area will therefore often summarize what is happening between nodes, but not always. Some times plain text is represented, just to clarify things before the actual animation starts. See also F. above.

H. The 'Pause' button will stop the progress of the animation in the movie clip. However, if the current frame residuals on a movie clip within a movie clip (nested movies), then this movie clip will play until it finishes its own movie clip, and then it will halt. Tip: -Watch the frame counter.

I. The 'Play' button will start the animation in the movie clip. However, when a movie clip is loaded for the first time, it is necessary to pres play two times to play continuously ahead.

J. The 'Stop' button will stop the animation and reset movie clip. This will bring the play head to the beginning and also reset volume setting back to default value for the clip. Tip: -It is recommended that during playing that one should use 'Pause' button to stop the animation, and thereby not loose track of where the play head is currently resided.

K. The 'Step Forward/Backward & Pause' and 'Step Forward/Backward & Play' buttons will step over the current sequence, and respectively Pause or Play from the next sequence. (Labels in the ActionScript is used to decide the length of each sequence, and will therefore vary from movie clip to movie clip).

L. The 'Volume' slider bar can control the sound level of each movie clip. Note: The volume is reset to maximum when 'Stop' is pressed. It will also reset if the movie is started from beginning, this is not true if the step buttons are used to pass the beginning of the movie.

M. This area contains an almost invisible frame counter. This frame counter can be used to se the progress of each movie clip in progress. Tip: -Use this frame counter to see if the animation is running or stopped.

7.2 Tools

To make the Illustrator we chose to use off-the-self program tools, which makes this project easily extendable in the future. Before we chose the animation tool "moving pictures" we looked at tools we were familiar with, such as PowerSim for modelling dynamic systems. It was not suited for discrete modelling, and was discarded. Some more tools were investigated, before we finally chose Flash 5 from Macromedia Inc. To make drawings we chose CorelDRAW since we were a bit familiar with this product.

7.2.1 Flash

Since we had no previous experience with Flash 5 programming, a lot of information had to gathered before we started using Flash in a serious manner to produce any useful animations. To do this we used interactive lessons, tutorials, websites, Flash ActionScript reference guide etc.

Further more, we set up a few design requirements before we proceeded:

- The system should be adapted to 800x600 pixels screen size
- The use of vector graphics to reduce file size on movie clips
- Easy navigation in the Illustrator
- Graphical User Interface (GUI) with a simplistic layout
- Set frame rate to 12 fps
- Compatibility and usability of the Illustrator

The reason for using screen size 800x600 pixels was to reach more users than by using for example 1024x768 screen size.

The use of vector graphics reduces the file size compared to pixel graphics, and therefore we used CorelDRAW9 to produce and export Windows Meta Files (*.wmf-files) that can be imported into Flash-working-files (*.fla-files). When a flash file with a typically file size of 7-60 MB is compiled, it produces a *.swf-file in the size between 200-1400 kB. This swf-file is compatible with most web-browsers today. Furthermore this file can be made into a so called 'projector file', which is a standalone executable file that does not require a browser.

The navigation is based upon well-known button shapes from consumer electronics; play, stop, pause, step forward and step backward. These buttons are used to step between sequences in the movie clip. However, the menu was designed to be implemented so that it would not take up space when not in use, for instance when watching a movie clip. It has also features like drop-down menu and drag-and-drop movement.

The GUI was designed to have some known elements that are the same in almost every movie clip. These drawings are somewhat simplified to reduce the amount of objects involved, and since the AKA procedure is not directly involved in all of these, we combined RNC and Node B, and CN as one unit, and HE as one location. The UE is illustrated with a USIM (UICC-card) to distinguish where the AKA procedures are taking place.

The graphics throughout the movie clips is developed using familiar colours, text type, headers and footers. Some areas are highlighted to focus on the action in motion. Each item that is going to perform an action has to be programmed, but since the movie is moving along a timeline it is possible to place actions on the timeline itself as well. This is all done by Flash's own programming language called 'ActionScript'.

When we chose a frame rate of 12 fps, it is due to recommendations picked up from the Internet. This seems like a normal (default) speed for a movie clip. However this is changeable. It is for instance possible to change the main menu and thereby changing the properties of all the movies being loaded by this menu. This is due to the Flash technology; When the main menu is loaded, it is loaded into level 0 of the program, and when the main menu loads a second movie clip, this clip is loaded into level 1 and if this movie clip again, loads a third movie clip, this could be loaded into level 2 or higher and so on. Every level that is loaded gets the same properties of the root level (level 0).

7.2.2 CorelDraw

One thing Flash 5 is not well suited for is making the actual objects that should appear in the Illustrator, so it had to be supplemented with another tool. We realised after playing around with Flash 5, that vector graphics is preferred compared to any pixel graphics tools. We had some knowledge with Corel Draw 9.0 and it felt natural to choose this program from Corel Corporation.

Corel was as well used to create vector graphic images to the thesis. Every drawing is made using similar colours, shapes, and designs to make a uniform look in this thesis. These static drawings were not suitable to import into the illustrator, so the illustrator has a lot of specially generated drawings.

8 3G security issues

The principles and objectives of the 3GPP security is described in the 3GPP document TS33.120. This chapter lists these issues for further discussion in the next chapter.

The security principles of 3GPP is based on three principles:
- 3G security will build on the security of second generation systems
- 3G security will improve security of second generation systems
- 3G security will offer new security features and will secure new services offered by 3G

8.1 2G security elements to be retained

The security in 3G will build on the security of second-generation systems. Security elements within GSM and other second generations system that have proved to be needed and robust shall be adopted for 3G.
- Authentication of subscribers for service access.
- Radio interface encryption.
- Subscriber identity confidentiality on the radio interface.
- Subscriber Identity Module (SIM) as a removable security module.
- SIM application toolkit.
- User-independent security operations.
- Minimised trust of the Serving Network by the Home Environment.

8.2 Weaknesses in 2G security

Some of the security features of 2G systems have been found weak and should therefore be corrected in 3G.
- Active attacks using a false basestation.
- Cipher keys and authentication data are transmitted in clear between and within networks.
- Encryption of the user and signalling data does not carry far enough through the network to prevent being sent over microwave links.
- Possibility of channel hijack in networks that does not offer confidentiality.
- Data integrity is not provided.
- The IMEI is an unsecured identity and should be treated as such.
- Fraud and Lawful Interception was not considered in the design phase of 2G systems.
- The HE has no knowledge of how the SN uses authentication parameters for subscribers roaming in the current SN.
- 2G systems do not have the flexibility to upgrade and improve security functionality over time.

8.3 New security features and services

With 3G both new security features and security of new services will be introduced. The new service features could not be listed at the time of writing. However the environment in which these features are can be described. They can be characterised by, but not limited to, the following aspects. (Some of these features and aspects are listed in bullets below).
- Different service providers will appear like content providers; data service providers and HLR only service providers (virtual operators).
- UMTS will be preferred over fixed line communications.
- More and more services will be pre-paid instead of post-paid subscriptions.
- Subscribers will have more control over their service profile.
- Users will experience active attacks.
- Non-voice services will be more important than voice services.
- The terminal will be used as platform for e-commerce and other applications.

9 Discussion

This chapter will discuss both security implementations of the UMTS system and the Illustrator developed.

9.1 Security in UMTS

It is often depicted that security in mobile systems never will be as good as for other network systems. Why does a mobile system have imperfections? Is security getting better for each generation of a mobile system? How has this effected the development of 3G mobile systems? Have 3GPP (The 3rd Generation Partnership Project) taken some shortcuts in security issues?

Some of the security principles and objectives of chapter 8 together with other security related problems are discussed in this chapter.

9.1.1 UTRAN radio interface encryption

In GSM, the radio interface encryption is only between the Base Transceiver Station (BTS) and the mobile. Since many basestations are connected the Base Station Controllers by microwave links, the need for more secure communications between them are required. Microwave links are seldom ciphered (besides shift registers) so in UMTS the RNC must be responsible for confidentiality instead of Node B to avoid this weakness. This will increase the security over the microwave links, but they are still a weaker point than the Uu interface between the terminal and Node B.

The properties of WCDMA, the radio access technology of UMTS, are of such nature that the signal is 'hidden' with the background noise. The messages are sent in information packets that are coded in both time and frequency, in addition they are XORed with a spreading code, so the actual user data stream is difficult to eavesdrop. When the confidentiality protection is not activated between the Node Bs and RNCs, the user data streams can more easily be found in plaintext.

To increase the security in the radio interfaces in the UTRAN, integrity protection should always be activated. Another solution would be to apply network confidentiality so all connections would be secured.

9.1.2 Nodes that holds keys

The integrity and confidentiality protection is placed in BTS in the GSM system, but in UMTS this is moved to closer to the CN and thereby reduces the number of nodes that stores the cipher and integrity keys. When fewer nodes are handling the keys, it is much easier to control the use of them. But it still means that the VLR/SGSN must keep track of what RNCs have received, and keep track on when to delete them.

Whenever the user gets into a new VLR/SGSN area, the temporary identities of the user are transferred between the old and new VLR/SGSN. AVs that are stored may also be transferred and when the old VLR/SGSN sends these, it must delete its own copies of the AVs. Then it should also make the RNCs delete the keys stored.

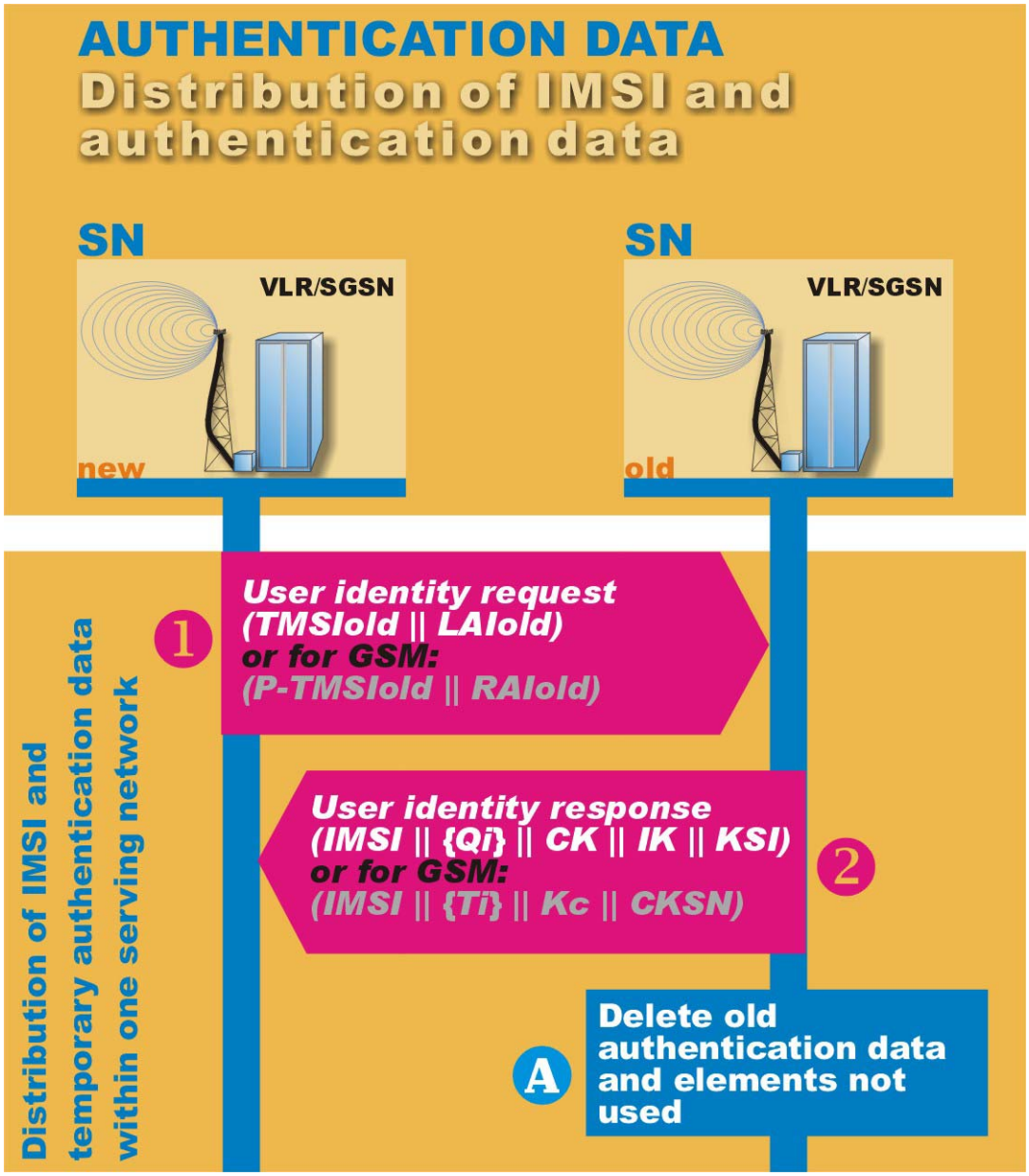

Figure 16 Distribution of IMSI and authentication data withing a SN.

By limiting the number of keys stored in the system, reduces the risk of unauthorized use. Because of this the responsible VLR/SGSN node should keep strict control over what RNCs it has given CK/IK keys to and make them delete them whenever they are no longer in use. It should also delete the AVs stored in its memory whenever they are no longer in use.

9.1.3 Authentication

Authentication of the user in UMTS is performed in a similar way of authentication in GSM. The problem with the false BTS in GSM is caused by the lack of user authentication of the network. By introducing a false BTS in the network, it can force GSM subscribers to use that BTS, but without any authentication or confidentiality. This means that the BTS is free of charge, but also that the communication is performed in plaintext over the air interface and in the BTS. By accessing the BTS the user data can be overheard.

In UMTS this is being avoided by introducing user authentication of the network. The AUTN message sent from the AuC to the USIM is authenticating the identity of itself. By doing this, the VLR/SGSN performing AKA shows that the user's HE trusts it. Since the integrity protection is not

optional, but required, it also helps to avoid problems with false BTSs. All signalling messages must be integrity protected and a handover to an unauthorised network will fail due to the lack of the IK.

The authentication of both users towards network and vice versa seems secure in UMTS, provided that the key generating functions are reliable.

9.1.4 User independent security operations

The security operations of UMTS are user independent. The USIM and Serving Network will automatically perform AKA and use integrity and confidentiality protection. This corresponds to GSM, but an extra feature is added in UMTS; user information of security services in use.

As stated earlier, integrity protection is always to be used for signalling messages in UMTS (except in some cases of emergency calls), but not for user data; and confidentiality protection is optional so the user should be informed whether or not this is being used. For some calls, the user might not care if confidentiality is not available, but with sensitive (e.g. online banking) transactions the service should not be able to perform without confidentiality protection activated.

The terminals should offer possibilities for user configuration of what services should be offered depending on different security services activated, together with a visual confirmation of this.

9.1.5 Data integrity

Integrity protection of user data is not provided in UMTS. This eases the processing load in both the UE and the RNC, and reduce message overhead. However when communication is not confidentiality protected, messages can be tampered with between the USIM and RNC. Tampering of messages that are confidentiality-protected will be detected at the receiver side and rejected, making higher-level protocols ask for retransmission.

Voice communication is easier to integrity protect, since the users may identify themselves by means of their voices. This reduces the need for integrity protection for voice calls. Thus the lack of data integrity, besides the existing indirect integrity protection of confidentiality protection, does not represent a problem, but confidentiality should always be used to provide indirect integrity protection for user data.

9.1.6 User confidentiality

User confidentiality is provided in UMTS by using temporary identities. Only the VLR/SGSN is supposed to know the connection between the user's real identity (IMSI) and the current temporary identity (TMSI). The RNC and Node B are only to know the TMSIs. The TMSIs are used over the radio interface towards the terminal, to keep listeners from finding out who is connected to the Node B. The IMSI is regarded a secret and should be treated as such. If a subscriber is moving around and the network performs handovers, the network nodes will interconnect and transfer the temporary identities between themselves to keep from revealing the true identity (IMSI).

Sometimes though, when the user connects to a SN, no temporary identities are available from the same network. This typically takes place whenever the user registers in a new SN for the first time, but can also occur if the nodes in the SN cannot resolve the temporary identity of the user by interrogation the other nodes. If this happens, the VLR/SGSN have to ask for the permanent identity (IMSI) of the subscriber and since no AKA procedures can be performed before the identity is known, the reply message from the USIM to the VLR/SGSN is sent in plaintext over the radio interface.

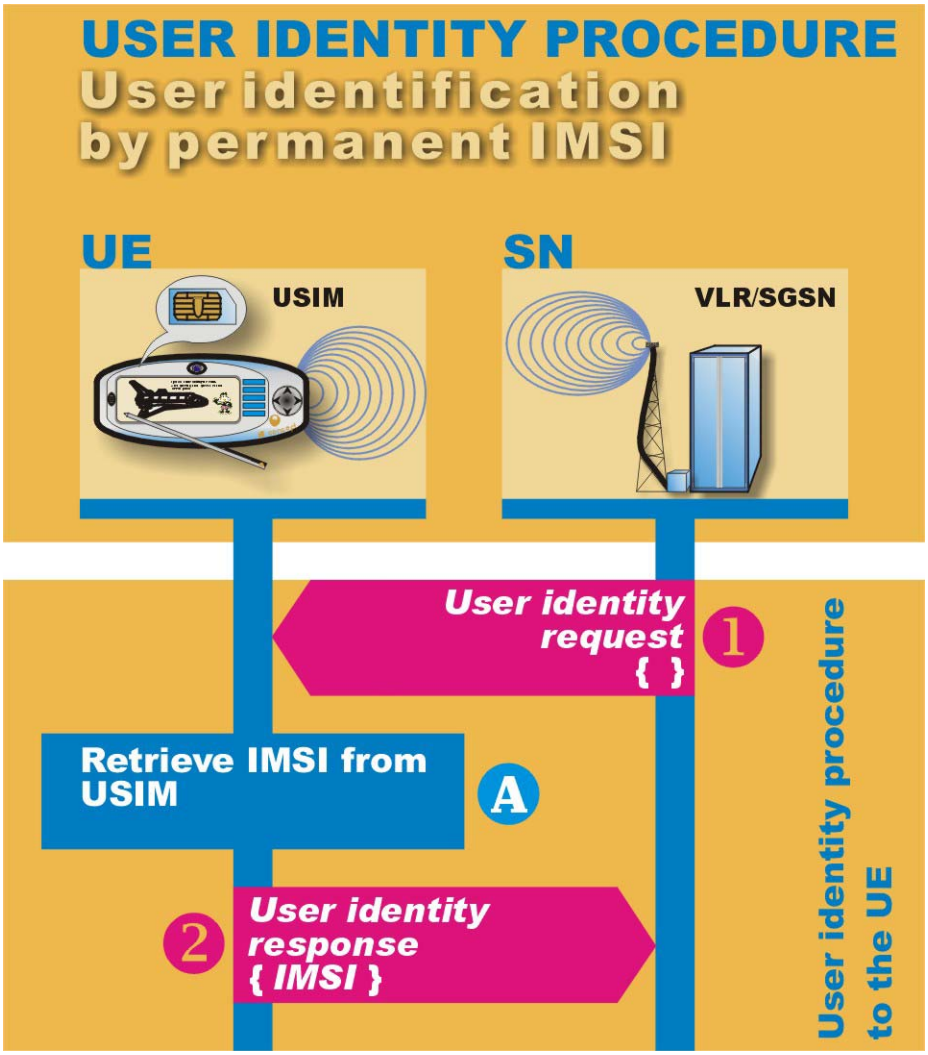

Figure 17 User identification by IMSI.

This represents the biggest security threat in UMTS. The only problem is that the USIM, to authenticate itself in another SN than its operator's network, have to provide a globally unique key to identify itself.

9.1.7 Threat of replay attacks

Replay attacks are attacks on the system where messages have been intercepted and then retransmitted (replayed) later. This if fairly easy to accomplish and will cause problems when using static data/input variables, so to overcome this threat sequence numbers (time variable inputs) are used.

Sequence numbers of AVs are introduced to prevent the serving network and others from trying to use it for multiple authentications and key generations. The only times messages can be used again are when the 'User authentication request' or reply is lost between the VLR/SGSN and USIM. This will make a timer elapse in the VLR/SGSN and make it retry the same 'User authentication request'

Functions f8 and f9 have their counters to prevent replay attacks. With separate counters for uplink and downlink, they may have the same values from time to time, but to keep from copy a message going one way and send it back the other way, a direction identifier is introduced. This makes sure that all messages will have unique (at least one different) input parameters.

The UMTS system seems secured against the threat of replay attacks.

9.1.8 Un-secured communication in CN

The communication between the nodes in the CN is not yet secured. The messages sent between them are therefore sent in plaintext. This makes eavesdropping on these links easy and both user data, signalling messages and AVs may be copied off these links. False operators may use the AVs to authorize and integrity-protect communication with a user, and un-trusted parties may just eavesdrop the user data on the links.

The 3GPP security group is currently working on a draft to introduce encryption between nodes in Serving Networks. But this is currently not in place and represents another big security threat of UMTS.

9.1.9 End-to-end encryption

Since the ciphering and integrity protection ends in the RNC, it may be tampered with throughout the CN. Some services require only being integrity protected between the terminal and RNC, but other more sensitive services must be kept confidential from end to end. To be sure of the integrity and confidentiality of the communication, end-to-end encryption should be introduced. With 2G narrowband systems, end-to-end encryption in real-time is hard to implement, but with wideband network common encryption solutions may be introduced. Both data and voice traffic can be encrypted and this will increase the personal safety of the users.

The regulators that want to use Lawful Interception procedures to tap the voice and data communications of the users may not appreciate being unable to interpret the communication, but it represents quite a security increase of the personal security of the users. The regulators will still have control over what numbers each users calls, where they are when they call and how long each call is, but will not be able to invade the privacy of the users by listening to voice calls or read the data sent and received.

9.1.10 Keys length

The keys lengths in UMTS are now up to 128 bits. This will surely be enough at the present time and in the near future. However, the ever-increasing computational power of computers is a factor to be taken into consideration. What seems to take forever to compute today may be done within an hour in a couple of years.

However we have not investigated this further, since the actual implementation of the key, confidentiality and integrity functions has not been a major focus in this thesis.

9.1.11 Anonymity at higher level services

When the AKA procedures have been performed, the user is identified towards the network, and the network knows where to send the bill for the service charges. With increased use of mobile as ‘debit card’ for paying (mostly) inexpensive services, like parking or vending machines, the user anonymity achieved by AKA should be retained, and the service providers should not care whether or not they know the identity of their customers as long as they get paid. As long as the user agrees to pay for these services, either by pre-paid or post-paid subscription, then there is no need to know who the user is.

The user’s UMTS operator should provide services that allow the user to charge his UMTS subscription for non-UMTS services. It should also offer the user possibilities to configure the services in such a way that he can acquire information about his current location, and still be anonymous to the higher-level applications. The user should be able to decline any service-provider applications that want to track user habits.

9.2 Illustrator

Flash technology is very popular and enabled for almost any available browser today. This enabled us to make an ‘Illustrator’ that could be viewed by most of today’s browsers, and in addition we could make executable files.

There are some limitations to whereas the menu system can be viewed as practical. The menu system was designed to be loaded as root level of the Illustrator, so that every other loaded movie would be loaded 'on top' of this, leaving the menu visible at all times. This would have been very practical; even though we failed in doing this 'movie clip loading procedure' the menu system was not abandoned completely. The menu system therefore inhabits a few extra features that are not directly useful in this version of the Illustrator. These extra features include drop-down and drag-and-drop menu.

Another small limitation is the incomplete online documentation on each object participating in the animations. The movie clips would have been more explanatory if every symbol could have a pop-up box with some information of their functionality. As everything is arranged now, the user has to fetch this report to get hold of such information.

One other aspect that would have made the Illustrator more interesting to work with is to implement a real simulation of the AKA procedures. A real simulation would be to generate keys and sending them between the objects in the animation. But this seemed to be a bit too much detailed compared to the level of in-depth details in the rest of the thesis. With a goal to show the logic of the AKA procedures, this was a natural choice to leave out.

The Illustrator shows both normal and special occurrences of the AKA procedures. The intention of the Illustrator was to give an easy-to-understand presentation of AKA with possibilities for the user to control the progress of the animations. This is done by using a simple navigation bar with Play, Pause, Stop and Step buttons.

It has been used simple features of Flash to keep the user focused on the important actions in the animation, instead of fancy graphics and solutions.

Most of the drawings used is designed especially for this illustrator. This is also the case for the music attached with the illustrator. All the music loops that are used are free-downloads from the Internet.

Conclusion

We have developed an illustrator of the Authentication and Key Agreement procedures in UMTS. It is successful in giving an easy introduction and explanation of the security features. By showing an animated version of the procedures, people without deeper knowledge of UMTS will be able to see which nodes that perform the AKA and the messages being exchanged.

One requirement for the illustrator was that it should be represented in a format that could reach most people with today's technology. To meet this requirement we chose to use the Flash technology, and the most common browsers on the market today supports this technology.

The thesis is a result of material picked from several relevant technical specifications and put together to a more comprehendible format. The thesis itself gives an introduction to the UMTS system and its nodes and their functionality, and that is in addition to any AKA explanations. When the illustrator is combined with this thesis it should give a well-arranged overview of the AKA procedures.

AKA procedures in UMTS have increased security compared with GSM. The new feature of two-way authentication eliminates the problem with false basestations. This is a very important security improvement.

Even though the security has improved in some areas, there are still security features that should be improved. It is not sufficient to just require integrity protection on signalling messages. All messages should be integrity checked, but indirectly by requiring confidentiality protection together with integrity.

AKA concept has been developed to perform authentication of the user and network, as opposed to 2G systems, which only authenticated users in a system.

References

[1] Harri Holma and Antti Toskala, WCDMA for UMTS, Wiley, 1. Edition 2000, ISBN 0-471-72051-8
[2] Harri Holma and Antti Toskala, WCDMA for UMTS, Wiley, Revised edition, 2001, ISBN 0-471-48687-6
[3] Øyvind Eilertsen, Security in UMTS – The KASUMI algorithm, Telenor FoU, R&D N 95/2000
[4] Aamodt T E, Friisø T, Køien G and Langnes R, Security in UMTS – Authentication and Key Agreement, Telenor FoU, R&D N 67/2000
[5] Langnes R, Aamodt T E, Friisø T, Køien G and Eilertsen Ø, Security in UMTS – Integrity, Telenor FoU, R&D N 4/2001
[6] Friisø T, Køien G, Langnes R, Aamodt T E and Eilertsen Ø, Security in UMTS – Confidentiality, Telenor FoU, R&D N 81/2000
[7] The Wassenaar Agreement on export controls for conventional arms and dual-use goods and technology. http://www.wassenaar.org/
[8] ETSI SAGE Task force for 3GPP, General report on the Design, Specification and Evaluation of The MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generating Functions, Version 1.0, Internal document
[9] 3GPP, Security Architecture, 3GPP TS 33.102 v3.7.0 (2000-12)
[10] 3GPP, Integration Guidelines, 3GPP TS 33.103 v.3.4.0 (2000-10)
[11] 3GPP, Cryptographic Algorithm Requirements, 3GPP TS 33.105 v.3.6.0 (2000-12)
[12] 3GPP, Security Principles and Objectives, 3GPP TS 33.120 v3.0.0 (1999-5)
[13] 3GPP, A Guide to 3rd Generation Security, 3G TR 33.900, v1.2.0 (2000-1)
[14] 3GPP, Man-Machine Interface (MMI) of the User Equipment (UE), 3GPP TS 22.030 v3.4.0 (2000-10)

List of figures

List of tables

Text Abbreviations

2G	2nd Generation
3G	3rd Generation
3GPP	Third Generation Partnership Project
AK	Anonymity key
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
AUTN	Authentication token
BTS	Base Transceiver Station
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CDMA	Code Division Multiple Access
CS	Circuit Switched
DECT	Digital Enhanced Cordless Telecommunications
DRNC	Drift Radio Network Controller
EIR	Equipment Identity Register
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
HLR	Home Location Register
IC	Integrated Circuit
IK	Integrity key
IMSI	International Mobile Subscriber Identity
IMUN	International Mobile User Number
Kbps	Kilobits per second
LA	Location Area
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MAC	Message authentication code (encryption context)
Mbps	Megabits per second
ME	Mobile Equipment
MExE	Mobile Execution Environment
MSC	Mobile Switching Centre
P-TMSI	Packet TMSI
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PS	Packet Switched
PSTN	Public Switched Telephone Network
R99	Release 1999
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RR	Radio Resources
RRC	Radio Resource Control
RRM	Radio Resource Management
SAT	SIM Application Toolkit
SGSN	Serving GPRS Support Node
SIM	GSM Subscriber Identity Module
SQN	Sequence number
SRES	Signed RESponse (authentication)

SRNC	Serving Radio Network Controller
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
URAN	UMTS Radio Access Network
USIM	Universal Subscriber Identity Module
UTRA	Universal Terrestrial Radio Access
UTRAN	Universal Terrestrial Radio Access Network
VHE	Virtual Home Environment
VLR	Visitor Location Register
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network
WCDMA	Wideband Code Division Multiple Access
WWW	World Wide Web
XRES	EXpected user RESponse

Definitions

Authentication:
- A property by which the correct identity of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, HE or SN.

Bearer:
- An information transmission path of defined capacity, delay and bit error rate, etc.

Broadcast:
- A value of the service attribute "communication configuration", which denotes unidirectional distribution to all users (source: ITU-T I.113).

Cipher key:
- A code used in conjunction with a security algorithm to encode and decode user and/or signalling data.

Confidentiality:
- The avoidance of disclosure of information without the permission of its owner.

Core network:
- An architectural term relating to the part of UMTS, which is independent of the connection technology of the terminal.

Domain:
- The highest-level group of physical entities. Reference points are defined between domains.

Downlink:
- Unidirectional radio link for the transmission of signals from a UTRAN access point to a UE. Also in general the direction from Network to UE.

Drift RNS:
- The role an RNS can take with respect to a specific connection between a UE and UTRAN. An RNS that supports the Serving RNS with radio resources when the connection between the UTRAN and the UE need to use cell(s) controlled by this RNS is referred to as Drift RNS.

Handover:
- The transfer of a user's connection from one radio channel to another (can be the same or different cell).

Home Environment:
- The HE is responsible for enabling a user to obtain UMTS services in a consistent manner regardless of the user's location or terminal used (within the limitations of the serving network and current terminal).

Integrity:
- The avoidance of unauthorised modification of information.

Interface:
- The common boundary between two associated systems

International Mobile Station Equipment Identity (IMEI):
- An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the PLMN and shall be unconditionally implemented by the MS manufacturer.

International mobile user number (IMUN):
- The International Mobile User Number is a diallable number allocated to a UMTS user.

Iu:
- Interconnection point between an RNC and a CN. It is also considered as a reference point.

Iub:
- Interface between an RNC and a Node B.

Iur:
- A logical interface between two RNC. Whilst logically representing a point to point link between RNC, the physical realisation may not be a point to point link.

MExE SIM:
- A SIM that is capable of storing a security certificate that is accessible using standard mechanisms.

Node B:
- A logical node responsible for radio transmission / reception in one or more cells to/from the User Equipment. Terminates the Iub interface towards the RNC.

Packet:
- An information unit identified by a label at layer 3 of the OSI reference model

Packet data protocol (PDP):
- Any protocol which transmits data as discrete units known as packets, e.g., IP, or X.25.

Public land mobile network:
- A telecommunications network providing mobile cellular services.

Radio Network Controller:
- This equipment in the RNS is in charge of controlling the use and the integrity of the radio resources.

Radio Network Subsystem:
- Either a full network or only the access part of a UTRAN offering the allocation and the release of specific radio resources to establish means of connection in between an UE and the UTRAN. A RNS is responsible for the resources and transmission/reception in a set of cells.

Release 99:
- A particular version of the UMTS standards produced by the 3GPP project.

Roaming:
- The ability for a user to function in a serving network different from the home network.

Security:
- The ability to prevent fraud as well as the protection of information availability, integrity and confidentiality.

Service:
- Set of functions offered to a user by an organisation.

Serving Network:
- The SN provides the user with access to the services of home environment.

Serving RNS:
- A role an RNS can take with respect to a specific connection between an UE and UTRAN. There is one Serving RNS for each UE that has a connection to UTRAN. The Serving RNS is in charge of the RRC connection between a UE and the UTRAN. The Serving RNS terminates the Iu for this.

Signalling:
- The exchange of information specifically concerned with the establishment and control of connections, and with management, in a telecommunications network.

Soft Handover:

- Soft handover is a category of handover procedures where the radio links are added and abandoned in such manner that the UE always keeps at least one radio link to the UTRAN.

Terminal:
- A device into which a UICC can be inserted and which is capable of providing access to UMTS services to users, either alone or in conjunction with a UICC.

UMTS IC Card:
- An IC card (or 'SmartCard') of defined electromechanical specification which contains at least one USIM.

UMTS network:
- Network operated by a single network operator and consisting of UTRAN access networks (WCDMA and/or TD-CDMA), optionally GSM BSS access networks, an UMTS CN.

Universal Mobile Telecommunications System (UMTS):
- The telecommunications system, incorporating mobile cellular and other functionality, that is the subject of standards produced by 3GPP.

Universal Subscriber Identity Module (USIM):
- An application residing on the UICC used for accessing services provided by mobile networks, which the application is able to register on with the appropriate security.

Universal Terrestrial Radio Access Network:
- UTRAN is a conceptual term identifying that part of the network, which consists of RNCs and Node Bs between Iu, and Uu interfaces.

User:
- An entity, not part of UMTS, which uses UMTS services. Example: a person using a UMTS mobile station as a portable telephone.

User Equipment:
- A Mobile Equipment with one or several UMTS Subscriber Identity Modules(s).

User Equipment:
- A device allowing a user access to network services. For the purpose of 3GPP specifications the interface between the UE and the network is the radio interface.

Uu:
- The Radio interface between UTRAN and the User Equipment.