HØGSKOLEN I AGDER

Agder University College

Investigation of spatial exposure control in 3G cellular/wireless system in conjunction with access authentication

by

Sverre Andersen

and

Hallgrim Flatland

Masters Thesis in
Information and Communication Technology

Agder University College

Grimstad, May 2003

Summary

The number of services provided by the mobile system has increased in an amazing rate. Technology has been the driving part for services like SMS, Chatting, and lately the new MMS standard with mobile terminals and integrated cameras. As the technology evolves, so does the mobile terminals and the services with them. The hype for the next decade may be position aware services. As GPS modules are getting cheaper, and more and more terminal providers integrate this chip with their equipment, the usage of such applications will explode. In the eyes of the security conscious operators, this new technology has potential for use in security systems. The 3G systems today offer exposure control on two dimension, i.e. usage (KB) and time. A new dimension is presented in this thesis, namely the spatial dimension. Based on the position of the user it is possible for the operators to control the user's access and keep an eye out on dubiously roaming partners. This thesis implements a spatial dimension to the authentication and access part of a 3G system. The results of the work show that the authentication and key agreement procedure may not be the most suitable place to implement such a system. Is it more favorable to implement is against the service?

Preface

This master thesis is part of the “Master of Science” degree in Information and Communication Technology at Agder University College in Grimstad. The assignment is the final stage in the education that leads to this degree. The work has been carried out in the period between January and May 2004.

The thesis is part of the “mobile student”-program at Agder University College. The program is cooperation between Agder University College and The Research Council of Norway, the sponsor of the program.

We would like to thank our supervisor, Assistant Professor Geir Køien, for valuable help and inspiration during the project period.

I would like to dedicate this master thesis report to my wife to be, Hilde Kristin. You have been incredible patient and loving through this entire period. Forever yours. Hallgrim.

I would like to thank my girlfriend, Nina. You have been a loving and caring person regardless of my long working hours. Thanks! Sverre.

Grimstad, May 2004.

Sverre Andersen and Hallgrim Flatland

Table of contents

Figures

Tables

1 Introduction

1.1 Background

Not long ago making a call was the only use of a mobile terminal. Nowadays, the number of available mobile applications grows fast. The number of applications serves large specter of different services. It is possible to file one's tax return, pay for parking or cinema using the mobile terminal. It is even possible to keep track of people's whereabouts using so-called "friend"-services. A large portion of the new services are closely linked to the user of the mobile terminal. Some sort of user identification is therefore needed to keep record of use and payment. The pre-shared secret stored on the USIM inside the mobile terminal acts as user identification and enables operators to bill for used services. A pin-code ties the user to the USIM. The growing number of mobile applications forces both users and operators to protect themselves and their interests from external threats. It is not in the interest of everyone to be traceable all the time. User identities are used over and over again and are known to a continuously growing number of service providers. It is in the interest of everyone to be sure that misuse of identities is avoided.

The number of services that depend on the current position of the mobile terminal is growing. The position data enables service providers to offer services that are adapted to the surroundings. As location services is about to become a commodity, the need for a spatial information grows. In order to provide location services the network and/or mobile terminal must be able to determine the position of the subscriber. The implementation of spatial information opens for new and interesting fields.

As the terminal is able to measure its position when using a service, it might be interesting to use this possibility in other areas too. Perhaps position can help to increase security in the mobile environment. To implement position as a spatial dimension in the authentication procedure is interesting. Such an implementation may make it possible to cross-check billing records received from serving networks. This way it is possible to link usage and position. The introduction of a spatial dimension in AKA opens new business concepts. The validity of areas can be decided either by the operator itself or in cooperation with the subscriber. It enables the operator to restrict use in areas that are considered to be vulnerable for the user.

The purpose of this thesis is to develop an experimental system implementing a spatial dimension in AKA. This system shall be used to discuss some of the questions regarding benefits and drawbacks of such an implementation

1.2 Thesis definition

The thesis will try to implement a spatial dimension in an experimental system.

The thesis title is:

> *Investigation of spatial exposure control in 3G cellular/wireless system in conjunction with access authentication*

The final definition of the thesis is:

> *The main goal of this master thesis is to develop an experimental system implementing a spatial dimension in 3G authentication systems. Benefits and drawbacks of adding this new dimension of exposure control shall be investigated. A theory of the sizes and measures of the critical variables, such as user speeds, exposure control update frequency etc, shall be developed. These theories shall be tested and verified using the demonstrator as far as possible. The results of tests like these may help the decision-makers in 3G wireless systems regarding policy issues.*

1.3 Report outline

This chapter gives a short introduction to the background of the master thesis, its definition and outline.

Position technology, trust and home control are some of the aspects that are discussed in chapter 2. A theory around the different parameters in a spatial system is also presented.

The demonstrator is presented in chapter 3. The chapter gives a description of system design, implementation and testing. A description of how messages are exchanged between entities in the demonstrator is given here.

Chapter 4 presents the results of the testing and verification of the parameter theory developed in chapter 2.

Chapter 5 discusses the results from chapter 4. Discussion of the benefits and drawbacks of such a system is also discussed.

Some concluding remarks are made in chapter 6.

2 Theoretical background

2.1 UMTS and UMTS Authentication procedure

The basis for this project is the UMTS Authentication and Key Agreement (AKA) procedure. It is a goal to not change it more than found necessary. This chapter will shortly present the UMTS architecture and the UMTS AKA procedure.

A 3G UMTS network consists of several nodes. They are listed in Figure 1. As a simplification, they can be categorized as user equipment (UE), serving network (SN) and home environment (HE). The UE consists of the mobile equipment, offering the radio interface, and a USIM representing the mobile subscription. The network is divided into access network and core network. The access network is called UMTS Terrestrial Radio Access Network (UTRAN), and consists of Node B and RNC. The core is divided in two, the circuit switch (CS) domain, and the Packet Switched (PS) domain. The CS domain consists of the MSC/VLR and the Gateway MSC (GMSC) providing speech services. The PS-domain consists of Serving GPRS Support Node (SGSN) and Gateway GSN (GGSN) providing packet switched data services. Every operator has a Home Location Register (HLR) and an Authentication Center (AuC), which is categorized as the Home Environment (HE). This is where all the information of the operator’s subscribers lay. For more information on UMTS architecture, see [3GPP TS 23.002].

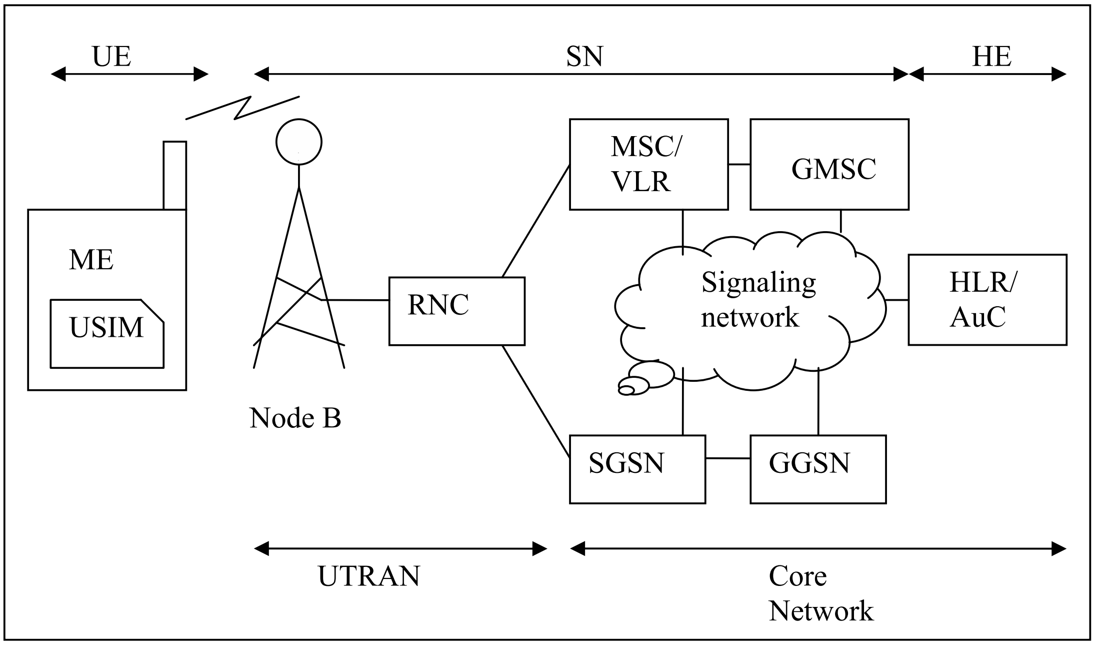


Figure 1 - UMTS nodes

UMTS AKA is a one-pass challenge response procedure with two-way authentication. This is in strong contrast with GSM authentication, which only offers authentication of user, not network.

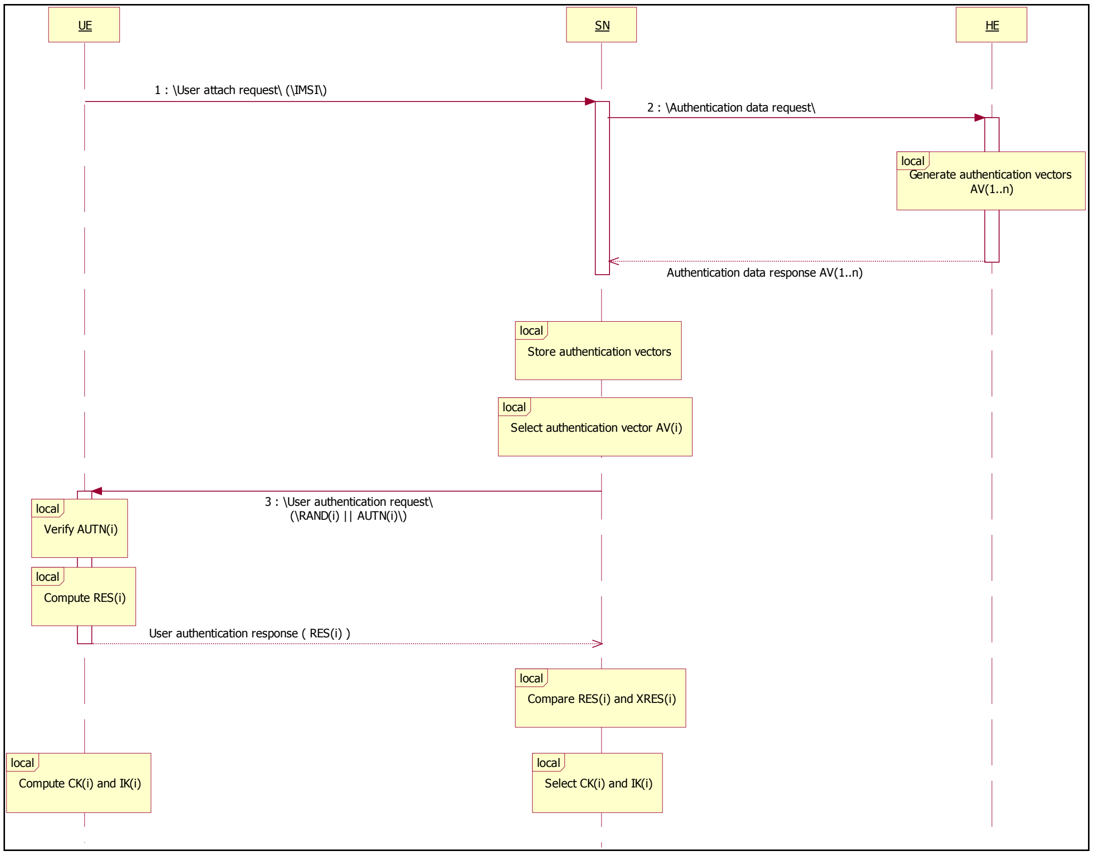

UE
SN
HE
1 : \User attach request\ (\IMSI\)
2 : \Authentication data request\
local
Generate authentication vectors AV(1..n)
Authentication data response AV(1..n)
local
Store authentication vectors
local
Select authentication vector AV(i)
3 : \User authentication request\ (\RAND(i) || AUTN(i)\)
local
Verify AUTN(i)
local
Compute RES(i)
User authentication response (RES(i))
local
Compare RES(i) and XRES(i)
local
Compute CK(i) and IK(i)
local
Select CK(i) and IK(i)

Figure 2 - UMTS AKA Procedure [3GPP TS 33.102]

Figure 2 shows the start of the attach procedure when a mobile user turns on the mobile phone. The figure is simplified. The actual AKA is done between USIM and SGSN/VLR. The encryption and integrity is actually preformed by the ME and the RNC. See [3GPP TS 33.102] for details.

The procedure starts with a phase where the UE send the IMSI to the SN. IMSI is an internationally unique identification of a subscriber. SN will then ask the HE associated with that IMSI for authentication data. HE generates the authentication vector based on a randomly generated sequence of bytes and a long-term pre-shared secret shared between UE and HE. The key is not sent with the data to SN. SN now sends a challenge to UE. The challenge includes the random number and an authentication token. The token holds the MAC that is used in the authentication of HE. UE now checks the MAC using the pre-shared secret and the RAND. If the check fails, UE rejects the network, terminating the procedure. If the check is ok, UE generates a response. The response is generated using the rand and the pre-shared secret. The RES is sent back to SN as a response to the challenge. SN compares the RES to the one received earlier in the authentication vector. If it matches, then the UE is successfully authenticated. The next phase for UE after sending a RES is to compute the keys used for confidentiality and integrity protection. SN uses the keys provided in the authentication vector.

2.2 Spatial AKA

In [Køien, Oleshchuk, 2003] a new dimension is introduced to AKA. They introduce a spatial mechanism directly incorporated in the AKA to, as they say, "improve the degree of control a home network has for a roaming subscriber". There are several ways position data can be used in conjunction with home control. The next two scenarios will give some examples on how this new type of control can be used.

Scenario 1

Subscriber control

Parts involved

Mobile operator	*/ Telesouth*
Subscriber	*/ Securitech Inc.*
Subscription	*/ Identified by IMSI*
User	*/ Employee at Securitech Inc.*

Case

Securitech Inc. has a lot of employers in the company. Some of them are equipped with a UMTS mobile terminal. This phone is intended for work-related use only. However, Securitech Inc. runs a sensitive business, and has to take many security measures in order to maintain their security goals. They can not allow their employers to use their mobile terminals in non-work-related actions. They are also very exposed to industrial espionage, and want to control their use of mobile terminals as much as possible.

Telesouth is a mobile operator with a well structured UMTS mobile network. They offer exposure control of the UE based on several dimensions. These are identity, usage, time and location. Time means that e.g. the user can only call for a maximum amount of time a day, or only between certain time intervals. The usage is measured in KB. The location dimension allows the owner of the subscriptions to define the areas where the subscriptions are allowed to be used.

There exists a contract between Securitech Inc. and Telesouth. In this agreement the UMTS subscriptions used by Securitech Inc. are defined. They define the times of day the subscriptions are to be used. Usually between 07:00 to 17:00. Some subscriptions for sales personnel are defined with no restrictions to time. The contract also defines the amount of data allowed to be downloaded per day. The last entry in the contract is map coordinates defining where these subscriptions are allowed to be used. Sales personnel traveling between different areas or even countries need another spatial acceptance area for their mobile subscriptions than employers that are only to be working at some factory or camp.

Scenario 2

Home control

Parts involved

Mobile operator	*/HE, Telesouth*
Access network owner	*/ SN*
Mobile subscriber	*/ company*

Case

The UMTS networks consist of Home Networks and Serving Networks. During the evolvement of UMTS, several actors have spawned and the scenario with few actors and where everybody trusted everybody is not applicable anymore.

Telesouth is a mobile operator with a well structured UMTS mobile network. They offer billing services of the mobile subscriptions based on several dimensions. Theses are usage, time and location. Time means that e.g. the subscriber is billed for the elapsed time during the use of the mobile network. The subscribers are also billed for the usage measured in KB. The spatial dimension allows Telesouth to verify bills being sent from other serving networks. Telesouth can keep tracking of where the subscribers have used their cellular phones with independent location data. The problem with criminal companies sending false bills can thus be minimized. Telesouth wants as much control over their subscriptions as possible.

As seen in the two scenarios, there are several ways a spatial dimension can be utilized. In scenario 1, the main goal was to restrict the use based on the location of the user. In scenario 2, the goal was to verify the usage to enable the mobile operators to protect themselves against criminal activity. Strictly tracking or monitoring the whereabouts of the user may also be wanted. Adding location data also raises some issues of privacy and trust. These topics are covered later.

[Køien, Oleshchuk, 2003] proposes a system based on 3GPP-WLAN AKA, which is a global AKA procedure. This project will look at the possibilities for adding such a mechanism in UMTS AKA, with as little change as needed. The problem of trust gives an extra challenge. Which entities can measure the position, and which entities can check the position against a database. How can the data be protected? How can privacy be preserved? [Køien, Oleshchuk, 2003] adds the actual sending of position data in the RAND part of the AKA procedure. This is possible due to the postulate that the Area Descriptors are at least the size of the native authentication area. One can separate the position checking into two phases. One phase is performed during authentication phase. The other phase is during rechecking. By using keys exchanged during the AKA procedure, and by encrypting and integrity protecting the data upon sending, the position exchange is bound to the current AKA procedure. By adding the second phase it is possible to have an Area Descriptor independently of the coverage of the current access network or native authentication area.

2.3 Home Control and Privacy

2.3.1 Home Control

There were only a few operators in the beginning of European mobile systems. Most of them were large national operators considering each other to be trustworthy. Home control is about protecting home operators against visited operators and need for such functionality was not present. The issues of home control were therefore not a deciding factor when developing GSM AKA. The same mechanisms were used as basis when developing UMTS AKA, a one-pass mutual identity authentication mechanism. It is considered to far superior its predecessor. The two-phased model with delegated responsibility is kept though. This is regrettable as that design is based on trust relations no longer considered to be realistic. The number of operators has exploded and not all of them are considered trustworthy. The authentication procedure is handled by SN, based on the assumption that SN is trustworthy. That does not longer have to be true. It is hard to justify such blind trust in other operators.

The UMTS AKA does not provide the operator with many options for home control. The network is interested in where the subscriber is located. The operator would also like to have some degree of spatial control when users roam onto other networks. The interests of the operator and the subscriber are conflicting. The user is concerned about his or her privacy and how gathered location data is used [Køien, Oleshchuk, 2003].

2.3.2 Privacy

It is possible to track most moving entities at high accuracy. This opens for useful services, but raises the need for addressing privacy issues. Privacy issues regarding development of location-based technologies and services. The potential of misuse of such technology is present. The subscriber's personal location privacy is therefore an important issue during development of these services.

People have different concern about being tracked. Investigations presented in [Barkuus, Dey, 2003] show that people are less concerned about their location being tracked as long as they find the service useful. The user finds it important to know who has knowledge of their location and when it is collected. The study rated position-aware services as less intrusive that the location-tracking ones. This supports the perception that people are more concerned when others can track their location than when their mobile terminal reacts to its own location.

A user related study is presented in [Ackerman, 1999]. The study shows that the users concern for privacy depends on what types of information they are asked to give up, but the applications usefulness to the user has an impact too. Most people are not opposed to providing location information in case of an emergency, but they are concerned about misuse. Users want to be able to avoid unwanted inquiries and intrusions. Eventually it is the users that needs to have confidence in a system for it to be successful, hence it is important to focus the attention on user privacy.

2.4 Trust

2.4.1 What is trust?

Trust impacts all our interactions with people and technology in different ways. Trust can be understood in terms of two dimensions: belief and dependence. Belief in someone is related to confidence, in addition to holding expectations about their behavior and intentions. Dependence, on the other hand, means that we trust someone we are not completely in control of. We need someone to behave in a certain way, and rely on them to do so. If we trust another person, we believe the person is competent and expect him to behave according to certain norms or rules. We depend on the person and hold him responsible for his actions.

In the world of UMTS, trust between different operators, i.e. Home Network and Serving Network, is accomplished by roaming agreements. A roaming agreement outlines the terms and conditions under which the participating companies will provide wireless service to each others subscribers. Roaming agreements are used where no company can offer complete national and international coverage.

2.4.2 Trust model entities

The presentation of trust model entities is restricted to the three key entities: the user, the home environment, and the serving network. Figure 3 includes a system model with only three roles and their trust relationships.

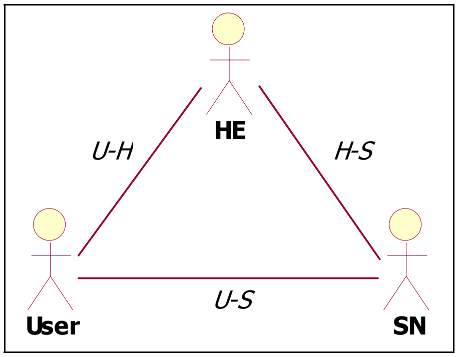


Figure 3 - Trust model entities

HE is the mobile system operator. HE keeps a record of subscribers and their authentication data. Authentication data is delivered to SN on request as SN is trusted to execute the authentication process. User is assumed to be a subscriber of HE. The user entity is represented by an application on a tamper resistant smartcard (UICC). In 3GPP systems this application is called USIM. In Figure 3 User also represents the user equipment, which the location measurement unit is a part of. SN is comprised by core network control entities which interface the access network. The trust between SN and HE, labeled "H-S", is based on roaming agreements or other partnerships. Physically, this trust can translate to a security solution for roaming [3GPP TS 33.234].

2.4.3 Trust Scenarios

To design and evaluate the implementation of a spatial dimension, the trust relations between the participants must be identified and divided into different scenarios. In a scenario where the spatial dimension is used, we have one home network (HN), one serving network (SN), and at least one subscriber. Scenarios of current interest are discussed in the following of this section.

2.4.3.1 Scenario A – The Serving Network Is Trusted

Figure 4 show that HE trusts SN with the respect to location information. Such relations normally rely on roaming agreements. If such an agreement is in place, a user may use another operator's access network. HE will authenticate him by using position information gathered by SN. Depending on which solution is chosen, the user may have to put trust in other, visited operators (SN), as well as in his home operator (HE).

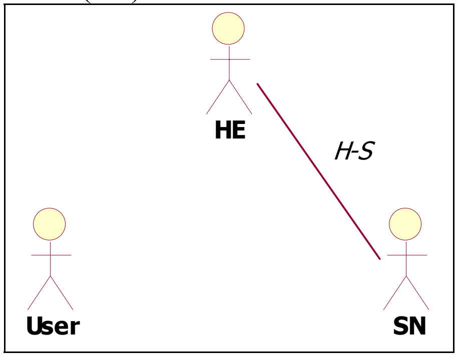


Figure 4 - The Serving Network is trusted

SN is in this scenario trusted with the respect of location information. No trust assumptions regarding User and location data are made. User should therefore be treated as an unreliable entity regarding such information.

2.4.3.2 Scenario B – When the User Equipment Is Trusted

Another scenario is when the UE is trusted by HE to provide location information. In Figure 5 User represents the UE, in which an LMU is located. A trust relation between the LMU and the USIM is present. USIM is issued by HE and there is a mutual trust between them. Since HE trusts USIM, HE also trusts the LMU. The trust relation between HE and USIM is based on a priori subscription arrangement. This trust consists of a long-term pre-shared secret stored securely both on User's USIM and in the operator's registers. The trust indicates a trustworthy exchange of data between User's terminal and HE. Because HE trusts User and User is trust LMU, a transitive trust between HE and LMU is present and data received from it.

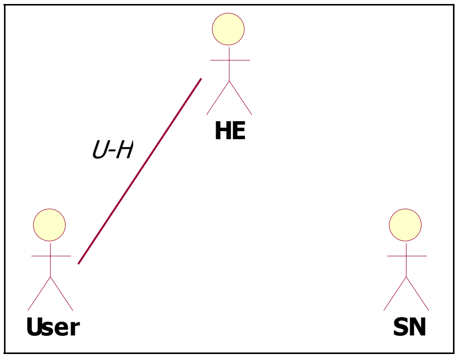


Figure 5 - The User Equipment is trusted

2.4.3.3 Scenario C – No trust relations between the entities

This scenario contains no trust relations between the entities regarding location information. There is no way that HE can determine a valid subscriber position.

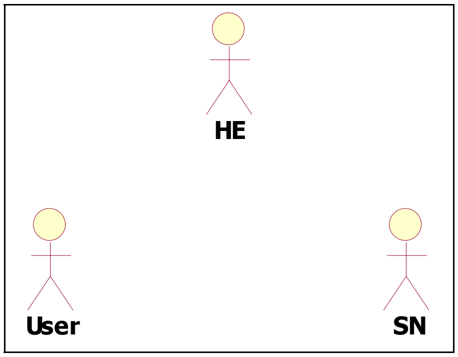


Figure 6 - No trust relations

The situation gets more favorable if we assume that SN and User act independently. Given that at least one entity tells the truth, HE will know that if both measurements correspond to the same area, then the spatial information is valid. On the other hand, if the difference between the given information is too large, HE has to accept that it cannot resolve the position of the subscriber.

If User is able to independently establish its position and if integrity between User and HE is established, one will have a situation where the User and HN does not need any trust in SN. Similarly, if HE can trust SN, HE does not need to trust User to be able to establish the position [Køien, Oleshchuk, 2003].

2.5 Positioning technology

2.5.1 Introduction

The focus on position technology in 3G cellular systems have increased the last few years. It escalated when the U.S. Federal Communications Commission (FCC) made a requirement for wireless Emergency calls; the Enhanced 911 (E911). The E911 was to be realized through two steps. During Phase I, starting April 1, 1998, it was required to resolve the callback number and the location of the cell site. Phase II, starting October 1, 2001, required the wireless carriers to resolve the position of a 911 call by longitude and latitude. The wireless carriers used network-based technologies to accomplish the positioning. The statistically requirements of the location accuracy were 100 meters for 67 percent of the calls and 300 meters for 95 percent of the calls. Subsequent technology provided handset-based solutions. Therefore on October 6, 1999, FCC adopted these new techniques and imposed location requirements of 50 meters for 67 percent and 150 meters for 95 percent of the calls [Hatfield, 2002]. The European Commissions (EC) E112 system in Europe is investigating the possibilities of having similar requirements [CGALIES].

Positioning systems are introduced to the cellular system as a requirement from the government. Positioning technology is expensive, and this would probably not have been introduced to the cellular systems for other services and used for a long time, had it not been for the E911 requirements.

2.5.2 Network assisted position technology

There are several technologies for determining a mobile terminal’s position. Most of them are based on using radio signals. Other techniques include using sight of view or sound waves combined with infrared light [Llusca, Val, Normand, Mercier, 2000]. All techniques presented here will have inaccuracy and uncertainties bound with them. Radio signals do not always follow a straight path to the receiver. A radio signal may be reflected and scattered when hitting mountains, buildings and other obstacles, hence the timing of a signals path does not represent the shortest path from the source to the receiver.

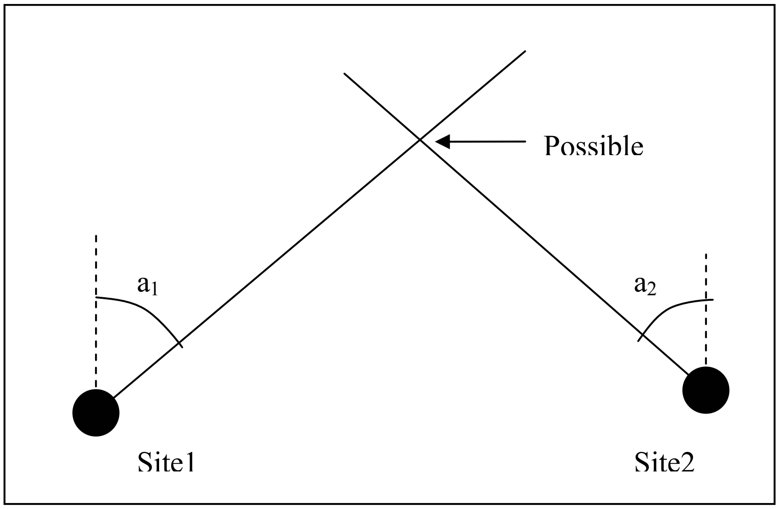


Figure 7 - Position determination using Angle of Arrival [Zhao, 2002]

It is possible to determine the angle of arrival (AOA) of a radio signal by using directional antennas or antenna arrays on the base station. The signal will be stronger in one of the sectors. By using the information from at least 2 base stations, it is possible to triangulate the angles, and pinpoint the mobile terminal's relative position. By combining that with the knowledge of the base stations positions, you get the absolute position of the terminal.

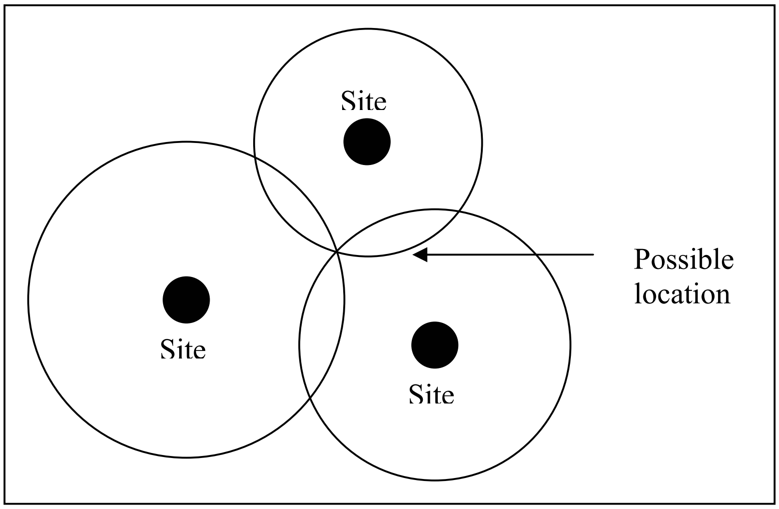


Figure 8 - Position determination using Time of Arrival [Zhao, 2002]

It is also possible to use what is called the time of arrival (TOA). By measuring the propagation delay of the radio signal, it is fairly easy to calculate the distance between the phone and the base station. By dividing the time delay by the speed of light, you get a circle around the base station where the phone will be positioned. Using 2 base stations, you get two points where the two circles intersect. The ambiguous result can be further clarified by using a third base station, or by ruling out the point that is certainly wrong. E.g. if one point happens to be located 200 meters deep inside a mountain where there is no radio coverage, you can rule that one out.

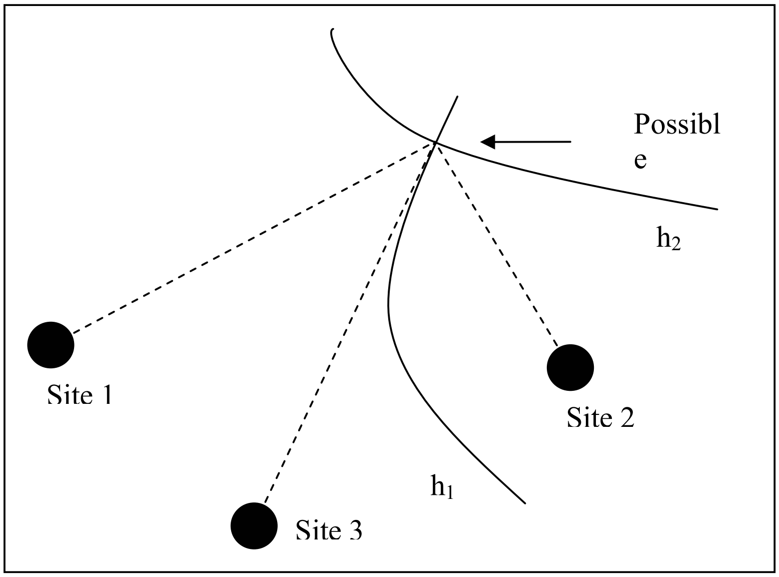


Figure 9 - Position determination using Time Difference of Arrival [Zhao, 2002]

The TDOA technique exploits the time difference of arrival of the signals from several base stations. By using mathematics, you can calculate a hyperbolic line between two base stations where the terminal will be located. By using at least two pairs of base stations, you can pinpoint the terminal's position where the hyperbolic lines intersect. This system requires either precisely synchronized watches or a means to calculate the time differences. Otherwise a 1 microsecond timing error could lead to a 300 m positioning error. There are some other location methods as well. The simplest is perhaps the Cell-ID method. If it is known which base station the caller is using, by knowing the coverage area of that base station, you also have knowledge of an approximate location of the caller. Whenever another method of measuring the location fails, this method can always be used. The accuracy of Cell-ID can be improved by combining other measurements like signal strength measurements or Timing Advance. It is possible to use other radio signals as well, such as AM/FM or TV signals. These signals have better coverage than those of cellular networks. Other methods include measuring the signal strength. You then need multiple cells to determine the location. You can also measure the signal characteristics patterns. These unique patterns may be stored in a central database for comparison. [Zhao, 2002]

2.5.3 Satellite based

The first operational prototype of the American NAVSTAR Global Positioning System (now called GPS) was launched February, 1978. This was after several predecessors like the Navy Navigation Satellite System (NNSS), the Timation system and the U.S. Air Force Project 621B. Today the total number of satellites launched, including spare satellites, is 24. They are distributed on 6 different orbital planes. The Russians have their own system called GLONASS (Global Navigation Satellite System). EU has started a similar program called Galileo. The first two test satellites are to be launched in 2005. The fully operational system will consist of 30 satellites (27 plus three spare) and is issued to be fully operational by 2008.

GPS is based on TOA. The satellites have synchronized atomic clocks onboard. They send a clock pulse towards the Earth. The GPS receiver then calculates the distance using the travel time of the radio signal. Using one satellite, you get a sphere around the satellite where the receiver can be situated. Using a second satellite, you get a circle where these two spheres intersect. A third satellite sphere will intersect the circle in two points. One point is probably not very likely to be the correct. Maybe it's way out in space. Then you can rule that one out, and the remaining point is the correct one. You can also use a forth satellite. This sphere will intersect one of the two points. It is not always enough for the positioning to be accurate to use many measurements. The extra measurements need to add extra information. Satellites that are situated almost at the same spot in the sky in proportion to the receiver will have almost the same errors. The angle between the satellites is important. The larger the angle, the more accurate the corrections, and hence the measurements, will be.

The clocks in the satellites are atomic clocks and very precise. They are also very expensive so you can not have an atomic clock in every receiver. By using a forth satellite you can correct the error in the time measurements. That way, each receiver becomes as precise as an atomic clock. The GPS system not only provides a way of measuring a position on the earth at a very high precision. It also provides a global synchronized time. The GPS satellites transmit on two different frequencies; L1 (1575.42 MHz) and L2 (1227.6 MHz). Each satellite uses these frequencies, but a special coding schema ensures that the signals can be extracted even during overlapping signals from different satellites. L1 is for civil use, and L2 is for military use only. [Kaplan, 1996]

Up until May 1, 2000, the L1 signal was applied with a feature called Selective Availability (SA). This would randomly degrade the accuracy of the GPS system. As stated in [The White House, 2002] this feature is today removed, and every civilian receiver can now reach accuracy within 10 meters.

2.5.4 Cellular wireless technology

One of the major problems with GPS as positioning technology is the need for view of sky. GPS can not be used for indoor positioning. This is a major problem, since people tend to spend a lot of their time indoors. They are indoors when at home and indoors when at work. A lot of research has been done to cover this gap. There are mainly two technologies used at this time. These are WLAN and Bluetooth. The general purpose use of these technologies has exploded through the last years. It seems natural to exploit existing infrastructure instead of developing and deploying new, expensive, single purpose systems. Most methods are based on Bluetooth (BT). By adding BT Access Points it will be possible to locate the terminals indoors. BT comes in three different power classes; 1 meter, 10 meter and 100 meters. E.g. by using cells of 10 meters, one can cover an entire hospital with an infrastructure of BT APs using a central server for the building for coordination. There are currently researches on different techniques using BT as positioning method. One is Cell-ID. Knowledge of which AP the terminal is connected to combined with the knowledge of where the AP is situated gives the position of the terminal. Another is using the signal strength and a third using signal characteristics pattern. This pattern must be stored in a central database for comparison. The technique of signal characteristics is also used for WLAN networks in [Prasithsangaree, Krishnamurth, Chrysanthis, 2002].

There has been done a lot of research in this area, but many questions stay unanswered. Who owns the infrastructure? Who uses the positioning data? What about privacy and securing the integrity of the data? What are the costs of building such systems? How can this be integrated with current 3G systems?

2.5.5 GRID system

Describing the terminal’s position and velocity requires a system to present these data. The earth rotates and an Earth-Centered Earth-Fixed (ECEF) Coordinate System is the better to use as coordinate system than for instance the Earth-Centered Inertial Coordinate System. The x-axis is fixed to 0° longitude. The y-axis is fixed to 90° E longitude. The z-axis is normal to the equatorial plane, pointing in the direction of the geographical North Pole. To be able to transform these Cartesian coordinates to latitude, longitude and height of the receiver, it is necessary to have a physical model describing the Earth.

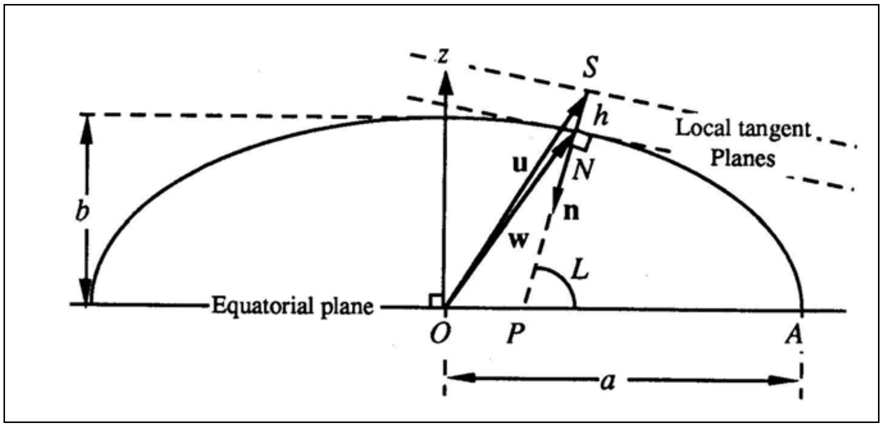


Figure 10 - Ellipsoidal model of Earth (cross-section normal to equatorial plane)[Kaplan, 1996]

The World Geodetic System (WGS-84) is the standard physical model of the Earth. It is based on that the Earths mass is not evenly distributed, but forms an elliptic shape. The equatorial radius is 6378.137 km. The polar diameter of the Earth is 6356.7523142 km. Cross-sections on the Earth parallel to the equatorial plane are circular. The height above sea level is calculated with respect with the reference ellipsoid. The local height above sea level can differ from the WGS-84. The latitude and height are defined using the normal on the ellipsoid at the user's receiver. Latitude is the angel NPA on the figure. N is the closest point on the reference ellipsoid to the user. P is the point where the normal to N intersects the equatorial plane
[Kaplan, 1996].

2.5.6 3GPP

Positioning is part of the 3G specification. UMTS R99 and R4 support Assisted-GPS. R5 also support Cell-ID and Observed Time Difference Of Arrival (OTDOA). These systems are based on either network measuring of position, or help from the handset [3GPP TS 25.305].

The information of Cell Identity, Service Area and the geographical coordinates are used in a Cell-ID based positioning system. It may seem attractive as positioning method, and it is. It's cheap and simple to implement, but it is not very accurate. The cell sizes of UMTS may be several km. That will not suffice for many services. The accuracy of Cell-ID can be improved by measuring the Timing Advance parameter. OTDOA can be performed both in the UE (UE-based method) and the network (UE-assisted). The distances to three different base-stations are required to make a position estimate. The time between a GPS is turned on, and until it is fixed to the correct satellites and correct position can be quite long. By using the information from GPS-receivers already fixed, this time may be significantly reduced. This is the basis of the Assisted GPS, where the access providers have position measurement equipment stationed throughout the network. The data transferred from the network to the UE will in addition to diminish the time to fix, also increase the sensitivity of UE's GPS. [Porcino, 2001]

Measurements show that OTDOA may achieve accuracy between 36-86 m in urban areas, and within 18m in suburban or rural locations (67% of the cases). A-GPS provides accuracy of 10 meters or better and is by far the most accurate measuring method. OTDOA has approximately the same coverage and accuracy for indoors use. A-GPS may not perform at all indoors unless certain techniques and assistance data are used. OTDOA is also cheaper to implement with only firmware updates required. A-GPS needs to install GPS chips in every handset [Porcino, 2001].

2.6 System Model

2.6.1 Introduction

Secure measurement and location verification is essential in systems that use current location as a parameter in the authentication process. Exchange of location data opens several issues. Who performs the position measurement? Who compares it to a record of valid areas? A system model will help to resolve these questions. Description of chosen technologies and possible limitations regarding these will be discussed. The system model shall also reflect on how the spatial dimension should be implemented in the authentication and key agreement.

2.6.2 Requirements

The project description states the goals of this thesis. In order to reach these goals, the system model has to fulfill some requirements:

The position of the mobile terminal shall be measured using some sort of position measuring technology. Which one and which entity shall do the measuring?
Which entity shall validate the position of the terminal against a record of valid areas?
The position of the mobile terminal shall be implemented as a spatial dimension in a 3G authentication system. How?
How can location privacy be preserved?

2.6.3 Available models

Different trust scenarios are discussed in chapter 2.4.3. What distinguish these scenarios are the trust relations between the involved parties. Each scenario will affect how the system chooses to exchange positioning data..

HE is not able to measure the position of UE by itself. Position measuring is therefore left for SN or UE to do. There are two ways to measure UE's position. The position can be resolved UE-based or UE-assisted. UE-based indicates that UE does the measurement itself using a positioning device in the terminal. When the position information is gathered, it is forwarded to the entity responsible for comparing it against valid positions. UE-assisted measurements means that UE assist SN while measuring the position, e.g. returning a radio signal as described in 2.5.2. The position data is forwarded to the visitatorial party. UE and SN are consequently both able to resolve the position of the terminal; hence it is possible for them to help each other out too. E.g. UE may ask SN for assistance if no GPS device is present or it is out of range. It is also possible for both of them to do the measuring. HE then has to check the measurements. If no trust relation regarding position is made, HE could take a considered decision, as the position is measured by two independent parties.

A record of valid areas (VA) is needed in order to figure out whether a measured position is valid or not. A record of such kind will be developed by the operator itself or together with the subscriber. There are different ways to check the position of UE against this record. First, the position information can be forwarded to HE for verification. HE would then have to respond with the outcome of the verification. Second, HE can distribute the VA record on demand. E.g. SN could receive a VA record covering its service coverage area. SN is then able to check the validity of UE's position, if it is provided. The VA record is distributed to the SN in question, as UE roams between networks. Another possibility is to distribute the VA record to UE. UE can verify its own position, if it has knowledge about its position and has access to the VA record at the same time. The distribution can be based on the reported position. A request for a new record has to be done every time UE enters a region that is not covered by its current record. Distribution of the VA record may decrease the signaling load generated from the new dimension, as the verifications does not have to involve HE. Distribution will be beneficial in scenarios with a low amount of roaming. Severe roaming will have the opposite effect, since this will lead to an increased activity of distribution of VA records and the signaling load between SN and HE will increase.

Considering maintenance, a VA record should be stored at HE. It is easy for HE to verify a position when the record is under its supervision. All needed for verification is to supply HE with the position of UE. HE is then able to compare the provided position against the record, before responding with the result. New algorithms are needed to verify a position. It is easier to implement this in HE than issue new USIMs with this functionality implemented to the subscribers. Minor adjustments to the algorithm would be possible if the verification procedure is centralized in HE and not in every USIM. It might be favorable to distribute this in USIM too. UE is capable of processing such data amount and distributed systems scale better than centralized ones.

The intention with this thesis is to investigate the possibility to implement a spatial dimension in AKA. The position check has to be performed during the AKA procedure and use the appurtenant keys. One way to approach the problem is to implement the position as a parameter in an existing message. This way the AKA message exchange would not be altered. This way the number of messages in AKA are not changed only the some parameters in them. Another alternative is to develop a new set of messages to perform the position verification. This would make the AKA procedure a bit longer, but keep the well arranged organization.

If the VA record is distributed to SN or UE and covers the service area of SN, the exchange of VA record will only occur during the AKA procedure. A VA covering the coverage area of SN will ensure that it is impossible to enter an invalid area without changing SN. The AKA procedure is executed every time UE is attaching to a new SN, hence the position will be checked against the VA record for verification. On the other hand, the position check has to be carried out when entering an area not covered by the VA record, if the size of VA is less than the service coverage area. The position verification has to be performed repeatedly to assure the validity of the current position.

The home control increases by adding a spatial dimension to AKA. Different measures must be utilized in order to maintain the location privacy of the user. [Køien, Oleshchuk, 2003] presents an analysis and a solution to the problem where UE does not trust HE with respect in location privacy. The S2PLIP protocol shows that it is possible to achieve spatial control without compromising the location privacy. Further work needs to be done in order to come up with a complete solution. This is left for others to do as it is out of the scope of this thesis.

2.6.4 Model of choice

This thesis is based on the fact that SN is not trusted regarding position measuring; hence scenario B, described in 2.4.3.2 is of current interest. A scenario where SN is not trusted in the exchange and verification of position reduces the number of different approaches.

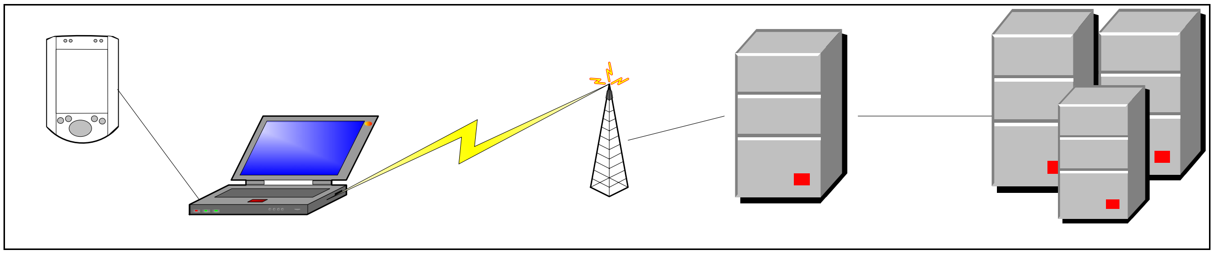


Figure 11 - Physical view of system

WLAN is used as radio technology to achieve mobile environment; hence the network is not capable of measuring the position of UE alone. A GPS device is selected as location measurement unit (LMU). A laptop will be used to simulate the UE. It will be possible for UE to measure its position by connecting the GPS to the laptop. Trust scenario B gives two possible solutions to validate the position; the position is validated by HE or by UE. UE needs knowledge about the VA record in order to validate its position. This means that that VA record has to be distributed to UE, based on its reported position. Instead HE is preferred to compare the reported position against the VA record. The VA record is stored and updated by HE, which makes it easy to do the verification there. The message exchange regarding position check is protected by encryption and integrity. A new set of keys is generated from values only known by HE and UE. This prevents SN from eves dropping or altering during the position exchange, even though every message is run through SN. Figure 12 shows how the position data is exchanged between UE and HE.

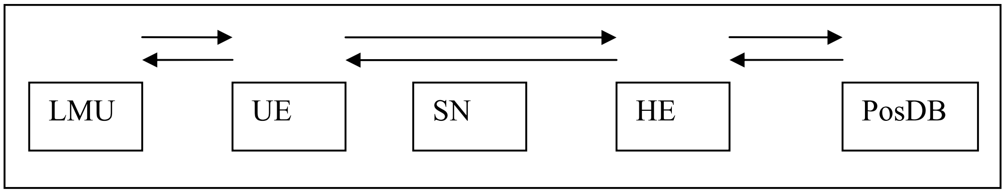


Figure 12 - Position exchange

The sequence starts by UE asking LMU for the current position. The position is forwarded to HE for verification as it is received from LMU. HE verifies the position by comparing it to the VA record stored in the position database (PosDB). HE will return a leasing time to UE if the position is reported to be valid. The leasing time is based on the distance from current position to nearest invalid area. Leasing time indicates how long to wait before executing the position check procedure again; hence assure that UE does not enter invalid areas.

The thesis state that a spatial dimension shall be implemented into a 3G authentication system. Our authentication system is based on UMTS AKA. In order for the position exchange to be considered as a spatial dimension, it has to be coupled with the appurtenant keys. This is achieved by adding an extra message exchange between UE and HE. The authentication procedure and position verification is described more thoroughly in 3.2.2.

2.7 Parameter settings and policy issues

2.7.1 Introduction

Adding a spatial dimension to the authentication routine of a mobile system can and will have consequences to both the users and the network owners. The users may experience to get locked out from using the mobile terminal based on their position. For this to work, the user may need to get warned in advance so he or she may take counter actions. E.g. the user may get a warning saying he or she will get locked out if continuing to move in the same direction and speed.

The spatial model chosen in chapter 2.6.4 depicts which entity that makes the decisions about position validity. The decision maker of the chosen model is HE. It is decided what to do and how to handle a situation when a user moves out of a valid area. This decision is based on the contract made with the customer. The customer is in this case an organization or a company owning a set of mobile subscriptions. The user will be the employer in such a company, using the phone on a daily basis. It is up to the company and the HE to agree upon a contract covering the company’s needs. E.g. the company may set up a contract saying that the mobile terminals should only be used within a certain city or campus, and that access should be restricted to only that area. It is also possible to grant access on a general basis, but be restrictive around certain objects or types of places. Here is an example;

> *A military company uses a PDA with a built-in UMTS phone and GPS. The PDA gives access to highly classified material. Besides other security measures as username and password and the fact that you need a USIM issued with correct IMSI and crypto-key, this PDA is equipped with a spatial authentication system. For security reasons, and to restrict the ability for the PDA to be compromised, it should only be used within the military camp. Access outside the camp should be denied.*

Spatial AKA may not only gain customers. HE may as well benefit from this feature. The main use may be the ability to monitor the users. For that purpose it may not be necessary to prohibit use, but merely monitor where the user was positioned while using the phone. This will give HE a means to verify the billing data given from different Serving Networks by a reliable source.

2.7.2 Parameters

There are several parameters to take into account when building a spatial system. HE needs to decide how to represent a position, how to represent validity areas, in what speeds a user moves, and how often a position check must be performed. The parameters of interest are listed in Table 1.

Table 1 - Parameters

Name	Description	Values ranges	Value used during testing
MAX_USER_VELOCITY	The maximum velocity a user is expected to achieve.	Max: 360 km/h Min: 0 km/h	36 km/h
LMU_DELAY	The update frequency of the location measurement unit.	Device dependant	Garmin etrex GPS: 1 sec.
SIGN_LATENCY	The maximum delay from when UE sends position data, until UE receives a response from HE. After this delay, a timeout will occur.	1 sec.	1 sec.
MIN_LEAS_TIME	The minimum time the UE uses to check it's position and check whether it's inside a valid area or not.	Max: INFINITE Min: LMU_DELAY + SIGN_LATENCY	2 sec.
LMU_ERROR	The accuracy of the location measurement unit. This is provided with each measurement.	System and conditionally dependant.	For GPS this lies around 10-15 m
MIN_AREA_SIZE	The minimum size of the validation area.	(MIN_LEAS_TIME * MAX_USER_VELOCITY) + LMU_ERROR	(2 s * 10 m/s) + 15 m = approx. 45 m

2.7.2.1 Velocity of user

One must calculate theoretical maximum and minimum speeds of a user. This is fundamental for setting other parameters such as position update frequency and size of validity area. The minimum velocity is of course zero. In such a case, it is theoretically not necessary to check the position more than once. The position has to be regularly checked to be able to detect that a user has started to move. The maximum velocity is a bit trickier to calculate. It is hard to predict how fast a user can move. There is a theoretical chance of a user moving at very high speeds. In practice it is probably enough to anticipate the fastest moving vehicle. E.g. maximum velocity can be set at 200 km/h for transportation by car or train. In a normal scenario, the user probably will be walking or standing still, with a speed of approximately 0-10 km/h. With a bicycle, normal speeds will be around 10-40 km/h. The radio technology also sets a boundary for maximum user speed. [3GPP TS 25.882] requires a mobile terminal in UMTS to work at speeds of 250 Km/h at frequencies of 2100 MHz. With today's requirements of the base stations, max speed is 155 km/h. For calculation convenience it may be suitable to set MAX_USER_VELOCITY = 360 km/h. By using WLAN for testing purposes, a pedestrian environment is assumed. It is more convenient to divide all measures and sizes by 10. Therefore the MAX_USER_VELOCITY is set to 36 km/h. The system is still applicable to a larger system, and the experience gained from testing will still be valid.

2.7.2.2 Position representation

The position is measured in many ways with varying accuracy. In this project a GPS receiver is used. The information provided is the time of measurement, the velocity of the user, the position of the user and the accuracy of the measurement. The time is represented as year, month, day, hour, minute and second UTC. The position is represented with the WGS84 datum in the terms of latitude and longitude. The altitude is measured in meters. The velocity is measured with a decomposed vector. It is showing both direction and magnitude of east-west velocity, north-south velocity and vertical velocity in the terms of m/s. The current horizontal position accuracy is also provided in meters.

2.7.2.3 Validity Area

Things to take into consideration when representing the validity area (VA), is shape and size of the polygon. There are two main things to take into consideration when choosing a shape of VA. First, adjacent VA's have to cover the surface, so no uncovered spots exists. There are several shapes with this property, e.g. squares, triangles or hexagons. [Køien, Oleshchuk, 2003] requires the VA to be at least the size of the native authentication area. Because the chosen spatial authentication model also performs position checks after the initial authentication phase, this is not a requirement in this paper. The VA can be freely chosen independent of the coverage of each access points. Secondly, it is crucial that calculations on the shapes, to determine whether a measured position is within a VA, are as fast and efficient as possible. This is to minimize the delay which in turns directly affects the leasing time. See chapter 2.7.2.4.

The easiest polygon to calculate whether a point is within the polygon's boundaries is a square or a rectangle. It requires only 4 calculations (top, bottom, left, right) in contrast of a hexagon needing many more calculations. What you are giving up by using a square shape, is the accuracy. The actual area to mark as invalid or valid may be shaped like a triangle. The inaccuracy by choosing a rectangle enclosing the triangle may seem less important than the benefits of choosing a simpler shape to do calculations on.

The chosen technique of measuring position gives three VA types or zones.

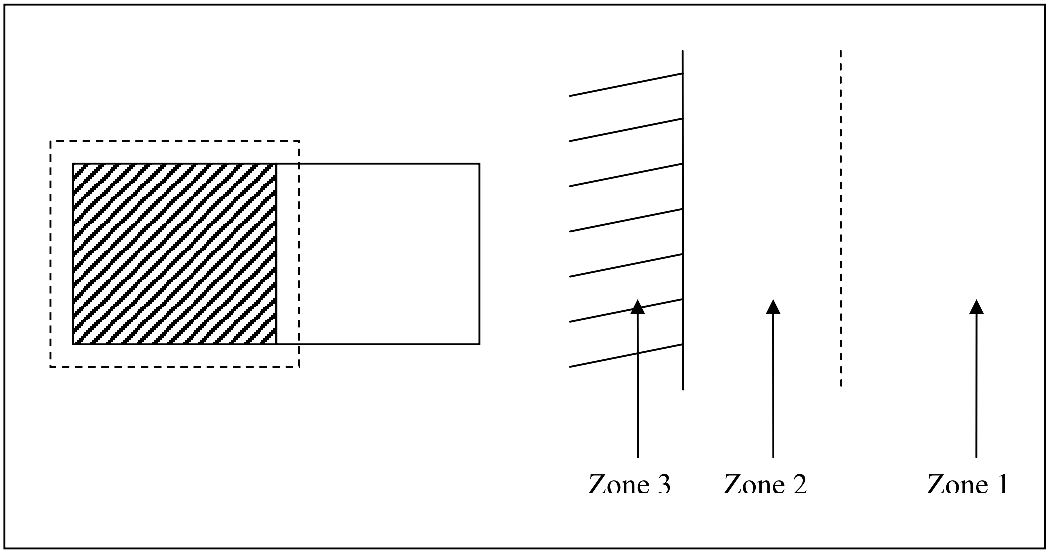


Figure 13 - Different zones in VA

- Zone 1: Grants 100 % access at all times.
- Zone 2: Possible to retain within area for a maximum period of MIN_LEAS_TIME. Access is denied if the position is measured within this zone.
- Zone 3: 100 % denial of access at all times.

By using a square as VA shape, there are some things to be aware of. As discussed in chapter 2.5.5, the shape of the earth is not round and certainly not flat. But; given a small section of a map it is acceptable to make this assumption. You can convert longitude and latitude directly to 2D Cartesian coordinates by saying latitude is Y-coordinates and longitude is X-coordinates. But you will encounter a problem when trying to convert this into meters. The distance of one degree in latitude is near constant throughout the entire earth. But the longitude distance gets smaller as you move from the equator towards one of the poles. Measuring the longitude any other place moving toward a pole you must multiply by the cosine of the latitude. Measuring the distance between two points can be done using the Great Circle Formula [Math World]:

$$[I] \quad Distance = ACos[Sin(lat1) * Sin(lat2) + Cos(lat1) * Cos(lat2) * Cos(lon1-lon2)]$$

The degrees must be converted to radians before inserted into formula [I], and the result must be converted back to meters.

The size of the validity area must be seen in conjunction with user speed, the accuracy of the position measurement and the position update frequency. The theoretical minimum size of an area is the same as the minimum size of zone 2.

$$[II] \quad MIN\_AREA\_SIZE = (MAX\_USER\_VELOCITY*MIN\_LEAS\_TIME) + LMU\_ERROR$$

With MAX_USER_VELOCITY set to 36 km/h and MIN_LEAS_TIME set to 2 seconds, the MIN_AREA_SIZE = 20m + LMU_ERROR.

2.7.2.4 Position check update frequency

The frequency of checking the user's position is realized with a leasing time given to the UE. Based on how far the UE is from the nearest edge of a false VA, the velocity of the user, and the accuracy of the position measurement, HE can calculate some probabilities of where the user will be the next time a position check is executed. Here is an example using MAX_USER_VELOCITY = 360 km/h.

> *The user is situated 1000 meters from the VA boundary. He is moving with a velocity of 5 m/s. This implies that the user may reach the boundary in 200 seconds, and HE gives a leasing time of 200 seconds to recheck the position once the user reaches the boundary. This will not work, since HE doesn't take into account all the parameters and uncertainty in the measurements, and the user may move into the false VA prior to the position check.*
>
> *HE must take into consideration the maximum speed the user may obtain within these 200 seconds. With the maximum theoretical speed at 360 km/h, and neglecting the time the user needs to accelerate from 5 m/s, the user may increase the speed and reach the boundary of the false VA within 10 seconds. In that case, HE should have given a leasing time of less than 10 seconds, not 200 seconds.*

There are more to take into consideration for HE. The position measuring device used in the example is a GPS. The accuracy of the GPS is given for each measurement, and sent along with the position data. Taking this into consideration, HE must assume that the user is situated several meters closer to the boundary than what is measured. Using the same parameters as above and an error of 10 meters, this gives a leasing time of 9.9 seconds, and is nearly neglect able. But what if this was removed from the calculations? An accuracy of 15 meters, which is often given as a mean for GPS accuracy, will in worst case scenarios lead to a user being allowed to move 15 meters into the forbidden VA for a short period of time. Or worse, what if the atmospheric conditions made the accuracy suddenly drop to 50 or 100 meters?

When the user is within a positive validation area all the time, there is no problem in execution of the spatial procedures. The problems arise when the user travels near or across the boundaries into false VA's. The leasing time must have restrictions in both ends. Based on maximum VA size, position measurement inaccuracy and maximum user velocity, there is a maximum leasing time. On the other hand, there is also a lower limit for leasing time. Leasing time of zero indicates that the position is not accepted. Theoretical lowest leasing time is the same as the technical possibilities of the position measurement unit plus the signaling latency. In our case, the GPS is measuring every 1 second. This means that a randomly picked measurement can take as little as a few millisecond, but also as much as 1 second at most. LMU_DELAY is set to 1 second.

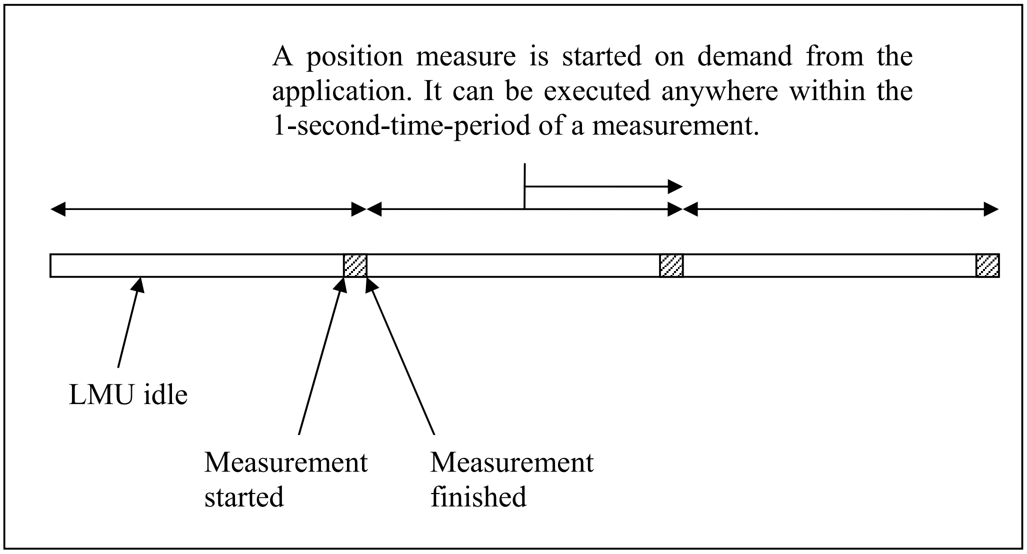

A position measure is started on demand from the application. It can be executed anywhere within the 1-second-time-period of a measurement.
LMU idle
Measurement started
Measurement finished

Figure 14 - Measuring position

The signaling latency must also be taken into account. This is reflected in the timeouts set for request-response signaling. A request for position check from UE to HE may take some time. If UE does not receive a response within a given time, the position check is considered to be false and UE is detached from SN. The timeout chosen is 1 second. This gives a MIN_LEASING_TIME of 2 seconds.

[III] MIN_LEASING_TIME = LMU_DELAY + SIGN_LATENCY

Setting the correct value of this parameter must be seen from two different points of view, i.e. the user and the network. If the network is to deny the phone to be authenticated based on spatial information, the user is probably aware of that. If so, the user could get warned in advance if he is moving towards an invalid VA. This will give the user a chance to stop the motion and stay within the positive VA. Seen from the network's point of view, it is desirable to monitor the user and of course provide the spatial service for its customers. The customer is in this case the company that owns the phone subscriptions. Sometimes it may be desirable to let the user enter such an area only making an entry in the auditory. This way the user may not suffer from getting outside of the boundaries, but still the company can get a report later. It's up to the company to apply corrections to the behavior.

If a user is standing still, the leasing time is still based on the distance to the nearest boundary to a negative VA. One can argue that the leasing time should be set to infinite, but that would not be correct. Then it would be impossible to detect that the user had started moving again.

When measuring outside of a positive VA, there should be a given interval for how often a re-authentication is performed. This should either be based on the last negative position check measuring the distance to a positive VA, or a defined time interval. It is not as crucial to grant access fast, than it is to deny access fast. In this project, the interval is set for 5 seconds.

2.7.2.5 Costs of adding spatial AKA

The extra position checking added to the AKA procedure will generate more signaling traffic. This means one extra roundtrip in the attach procedure, and one roundtrip for each position measurement after that. The amount of data sent is in the measures of 100 bytes per datagram. This may seem little with one user, but scaling this for use with thousands, this can not be neglected. It is desirable to keep the update frequency as low as possible to keep the signaling load at a minimum. The computational costs lie with the HE. HE must calculate which VA the user is within, and check all the surrounding VA's whether an invalid VA is within reach. Then HE must calculate the shortest distance between the user and that VA using formula [I]. And then calculate the leasing time with formula [IV].

[IV] Leasing Time = MAX [((Distance – LMU_ERROR) / MAX_USER_VELOCITY), MIN_LEAS_TIME]

3 Demonstrator

3.1 Purpose

The main goal of the master thesis is to develop an experimental system implementing a spatial dimension. First, the demonstrator shall investigate in it is possible to add a spatial information into the authentication and key agreement. Second, the purpose of this demonstrator is to create a test bed for testing the use of spatial information in authentication and key agreement. It shall be a concept demonstrator to investigate benefits and drawbacks generated by such an implementation.

The demonstrator shall log test data while testing the concept. This data shall be used to validate a theory of sizes and measures of critical variables, such as user speeds, update frequency and leasing time, developed in chapter 2.7. Conclusions from this investigation may be used as guidance when implementing this concept in real mobile systems.

3.2 Design

3.2.1 Use case

In addition to verify the concept, different use cases are developed for the demonstrator.

Use case A:
The user turns the mobile terminal on. He is located in an area defined to be valid. The terminal initiates the attach procedure. After the mobile terminal and the network have been authenticated the position of the terminal is checked and found valid. The terminal is attached to the network and is able to use its services.

Use case B:
The mobile terminal is turned on. The attach procedure fails as the position is reported to be invalid. It is not possible to use services provided by the network.

Use case C:
The attach procedure it completed successfully. A recurring procedure shall check the positions validity. The time between each check shall depend on the distance to nearest invalid area. A detach shall be initiated when the user travels into an invalid area. Both the service and network shall be detached.

Use case D:
The mobile terminal is located in an invalid area as it is turned on, hence the attach procedure will fail. The attach request procedure is repeated to assure that the user will be able to use services when they become available. The attach request will complete successfully when located in a valid area.

Different combinations of use cases will give a good indication on the applicability of the demonstrator.

3.2.2 Communication Protocols

3.2.2.1 Introduction

The scenario in question, described in chapter 2.4.3.2, contains three entities of interest; the user equipment (UE), the serving network (SN) and the home environment (HE). Chapter 2.6.4 shows how these entities connect with each other. For the network entities to be able to communicate, a set of communication protocols are specified. These protocols are developed and adjusted to suit this particular assignment. Existing protocols with equivalent functionality and specified by 3GPP, are used as foundation for these protocols. This chapter will give an insight in how these protocols has been adjusted to fit this assignment's needs, and which simplifications that has been made. The protocols has been divided into two sections on the basis of were their functionality is used.

3.2.2.2 Mobility Management

Generally the main functions of Mobility Management (MM) are registration, paging, location update, handover and rerouting. Only one SN is implemented in the demonstrator; hence paging, location update, handover and rerouting are not needed. The decision is based on the fact that the location update feature is not needed in order to demonstrate to concept. Low delay is important while transporting signaling protocols. A connection-less protocol, like UDP [RFC768], is therefore required. The fact that UDP provides no delivery guaranty is favorable, since the MM protocols do not have time to wait for a retransmission.

3.2.2.2.1 GPRS Mobility Management Protocol

Communication between UE and SN is implemented and specified in a protocol called GPRS Mobility Management Protocol (GMMP). Its main liability is to support the registration function of MM. GMMP is our simplified version of GPRS mobility management protocol [3GPP TS 24.008], specified by 3GPP. Only functionality needed to solve the thesis is specified and implemented.

Table 2 lists the vocabulary of the GMMP protocol. A comment to each message, its origin and end point is presented. The functionality of these messages is demonstrated and described in Figure 15.

Table 2 - GMMP Vocabulary

Message	Origin	End point	Comment
ATTACH_REQ	UE	SN	Initiates the attach procedure
AUTH_REQ	SN	UE	Request for authentication data
AUTH_RES	UE	SN	Response containing requested data
EID_REQ	SN	UE	Request for equipment ID (IMEI)
EID_RES	UE	SN	Response with requested IMEI
ATTACH_ACCEPT	SN	UE	SN allows UE to attach. Provides a P-TMSI for later use.
FORWARD	UE / SN	SN / UE	A bearer for transparent transmission of messages between UE and HE.
ATTACH_COMPLETE	UE	SN	Completes the attach procedure
DETACH_REQ	UE	SN	Request to detach from UE to SN
DETACH_RES	SN	UE	SN response on request to detach

3.2.2.2.2 Mobile Application Part Protocol

Mobile Application Part Protocol (MAPP) is used when SN communicates with HE, or vice versa. MAPP provides the needed mechanisms to communicate between SN and HE. MAPP is a simplified version of Mobile Application Part [3GPP TS 29.002], specified by 3GPP, containing functionality needed to communicate between the entities in the core network. The functionality of these messages is demonstrated and described in Figure 15.
The protocol vocabulary is formed by the messages listed in Table 3 along with origin, end point and comment.

Table 3 - MAPP Vocabulary

Message	Origin	End point	Comment
AUTH_INF	SN	HE	SN request the data needed to authenticate UE
AUTH_INF_ACK	HE	SN	Response with requested data from HE
CHK_IMEI	SN	HE	SN asks HE to check provided IMEI to its registers
CHK_IMEI_RES	HE	SN	HE's response after checking IMEI
FORWARD	SN / HE	HE / SN	A bearer for transparent transmission of messages between UE and HE.

3.2.2.2.3 Home Control Protocol

The position is exchanged between UE and HE using Home Control Protocol (HCP). This protocol consists of the two messages listed in the table below. HCP is transported over the FORWARD-message in GMMP and MAPP.

Table 4 lists the massages in HCP along with origin, endpoint and comment.

Table 4 - HCP Vocabulary

CHK_POS_REQ	UE	HE	UE requests HE to check its position
CHK_POS_RES	HE	UE	HE responds with granted leasing time

3.2.2.2.4 Interaction between GMMP and MAPP

A dialog between UE and SN is initiated, as UE is turned on. This is the registration function of MM. UE informs the network that it is ready to start sending and receiving communication data. The registration function also includes the process of authenticating the user. This process is generally referred to as the UMTS GPRS attach, in the UMTS specifications.

The following figure demonstrates the interaction between the network entities during the attach procedure.

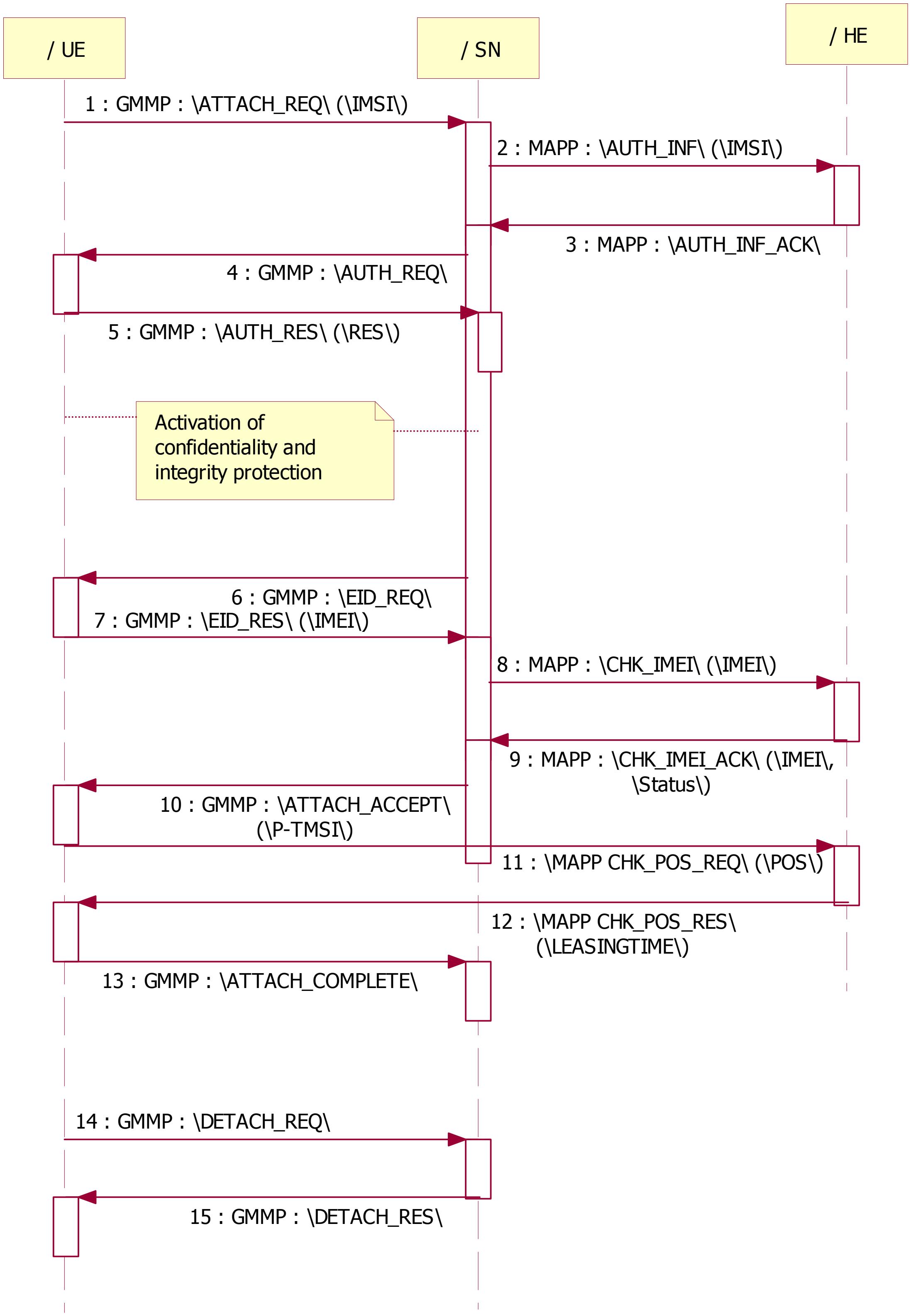

/ UE
/ SN
/ HE
1 : GMMP : \ATTACH_REQ\ (\IMSI\)
2 : MAPP : \AUTH_INF\ (\IMSI\)
3 : MAPP : \AUTH_INF_ACK\
4 : GMMP : \AUTH_REQ\
5 : GMMP : \AUTH_RES\ (\RES\)
Activation of confidentiality and integrity protection
6 : GMMP : \EID_REQ\
7 : GMMP : \EID_RES\ (\IMEI\)
8 : MAPP : \CHK_IMEI\ (\IMEI\)
9 : MAPP : \CHK_IMEI_ACK\ (\IMEI\, \Status\)
10 : GMMP : \ATTACH_ACCEPT\ (\P-TMSI\)
11 : \MAPP CHK_POS_REQ\ (\POS\)
12 : \MAPP CHK_POS_RES\ (\LEASINGTIME\)
13 : GMMP : \ATTACH_COMPLETE\
14 : GMMP : \DETACH_REQ\
15 : GMMP : \DETACH_RES\

Figure 15 - The attach procedure

SN must check the validity of the user and the identity of the mobile terminal, when SN receives a GMMP ATTACH_REQ from UE. It is possible to validate the user identity by combining the authentication data provided by HE (the authentication vector) and what is stored in the USIM. SN receives the authentication data from HE as a response to message 2 in Figure 15. The authentication procedure is successful if UE responds to SN with the corresponding answer. This leads to an activation of integrity which protects later signaling exchange between the mobile terminal and the network.

The terminal identity shall be checked. This is an optional procedure in UMTS [3GPP TS 23.060], but is implemented to be mandatory. SN asks UE to provide its IMEI (International Mobile Equipment Identifier), a unique 15-digit number, by sending EID_REQ. UE responds with an EID_RES containing the requested IMEI. SN asks HE to check the status of IMEI through EIR. IMEI is checked to assure that it is not stolen or to gather statistics on fraud or faults [3GPP TS 22.016]. The CHK_IMEI_ACK from HE indicates whether or not the terminal is allowed to use the network.

As both identities, user and equipment identity, are checked, UE is nearly registered with the network. The next step is for UE to receive a P-TMSI from SN. This is a temporary identity, which will be used in later interaction between UE and SN for enhanced security. In the demonstrator, the P-TMSI is simplified to be the same as IMSI. This will decrease the security in the system, as the real identification is sent each time. It is our opinion that such a reduction in security can be neglected in this demonstrator. The limited usage, operating time and numbers of terminals support this.

The current location of the UE has to be checked before the registration procedure is complete. UE sends its current location data to HE with a CHK_POS_REQ-message. The message is transported with the GMMP message, FORWARD. The CHK_POS_REQ-message is confidentiality and integrity protected. The keys used in this exchange are derived from K and IMSI. K is a secret key only known by USIM and HE. This ensures that it is impossible for SN to tamper with the data. The result of the position check is received inside a CHK_POS_RES-message. Leasing time larger than zero, indicate that the current position is allowed. The position check is a recurrent procedure. Leasing time indicates the time interval between each execution of the position check routine. Leasing time larger than zero triggers the transmission of ATTACH_COMPLETE from UE to SN. The attach procedure is complete. Otherwise, if leasing time is zero, a failure message is sent to SN. Both UE and SN return to their initial states.

The demonstrator implements one SN. With only one SN, the need for location update functions, like the GPRS location update procedure found in [3GPP TS 29.002], are not needed. Before the terminal is turned off, a detach request is sent to SN. A response is returned after releasing all resources related to the terminal in question. The purpose is to make it possible for SN to keep an up-to-date list of connected terminals. It is implemented similar to IMSI detach described in [3GPP TS 23.060], but with some simplifications. It is implemented as a UE-initiated procedure, as opposed to the implementation in UMTS where it can be initiated by both parties.

The complete message sequence shown in Figure 15, is mandatory. The keys used in encrypting and integrity protecting the CHECK_POS messages are derived directly from the authentication process. The mandatory sequence and the key material used couples the position checking with the authentication procedure.

It is possible that UE's attempt to attach to the network fails. A timer is initiated each time a request from one of the entities is made. If this timer exceeds a given value, hence a response did not arrive, the procedure is canceled. Then the only option is to start over again. The possibility of timeouts is discussed further in the next section. A request to register with an invalid IMSI or IMEI will be rejected, as these values are checked against records found in the network.

3.2.2.2.5 State diagrams

State diagrams are developed to keep track of which state each entity has at a given time. The entity state is closely related to the procedure it is processing. State diagrams also make it easier to foresee and control the upcoming events. It serves as a set of rules that describes the expected response on given actions. A received request and the transmission of a response is the general mechanism that triggers the states to change. The following diagrams give an insight in how the states of the different entities changes.

UE State

Figure 16, shows how UE changes state form one to another as the GMMP Attach procedure progress. The procedure is started when the mobile terminal is turned on. An ATTACH_REQ-message is sent from UE to SN. The AUTH_RES_SENT-state indicates that AUTH_RES is sent and that the next incoming message is an EID_REQ. When this request is received an EID_RES-message is returned. The UE-state changes to EID_RES_SENT. The next message for UE to receive from SN is the ATTACH_ACCEPT-message, indicating that the reported terminal identity is checked successfully. Now UE has to send its position to HE. This is done by sending CHK_POS_REQ. The response indicates whether the current position is allowed to connect from or not. A positive response sends an ATTACH_COMPLETE-message to SN. UE enters the ATTACHED-state and the GMM Attach request procedure is completed.

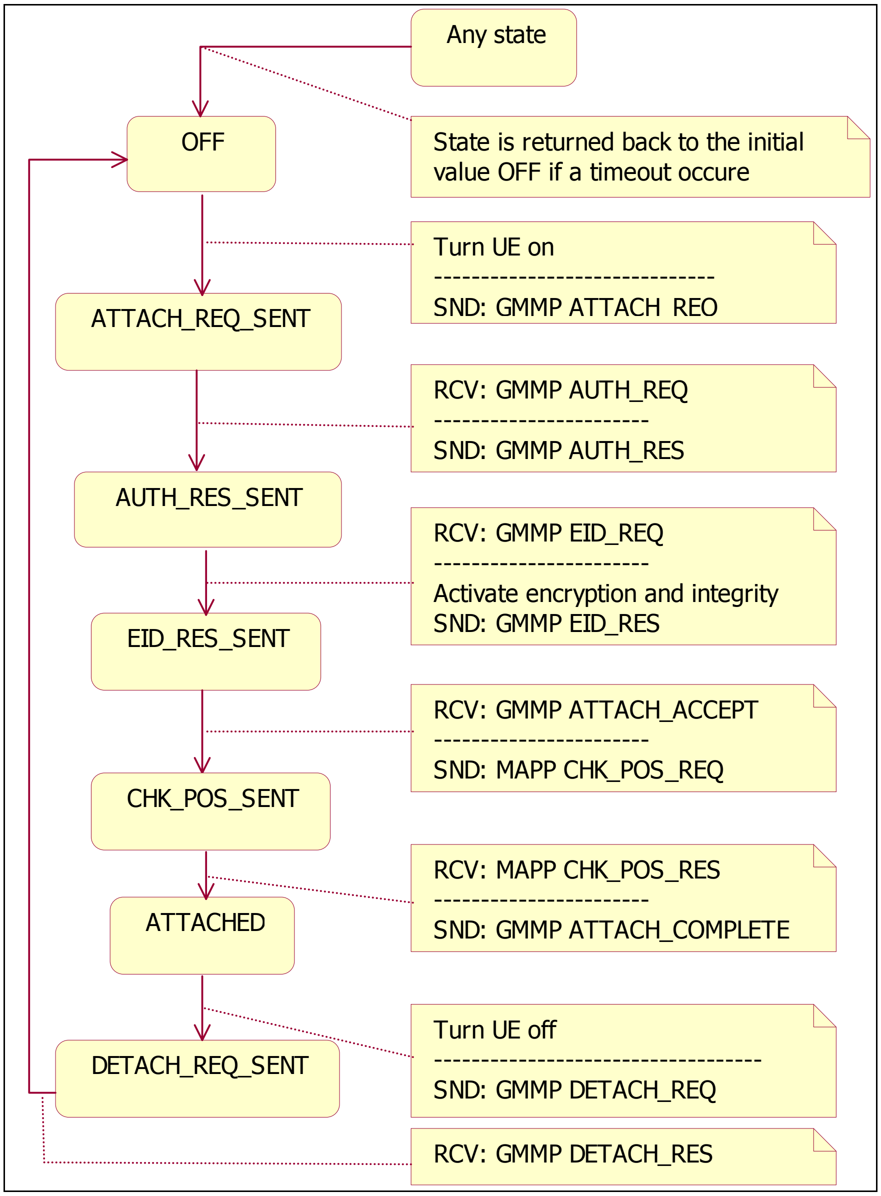


Figure 16 - UE state diagram

When UE wish to detach form SN, a DETACH_REQ-message is sent. After releasing used resources, SN responds with a DETCH_RES. UE is detached from the network, and all used resources at SN are released. UE enters the OFF-state, while SN is idle and ready to receive new connections.

SN State
Figure 17 is equivalent to Figure 16 and shows the states of SN during the GMMP Attach procedure.

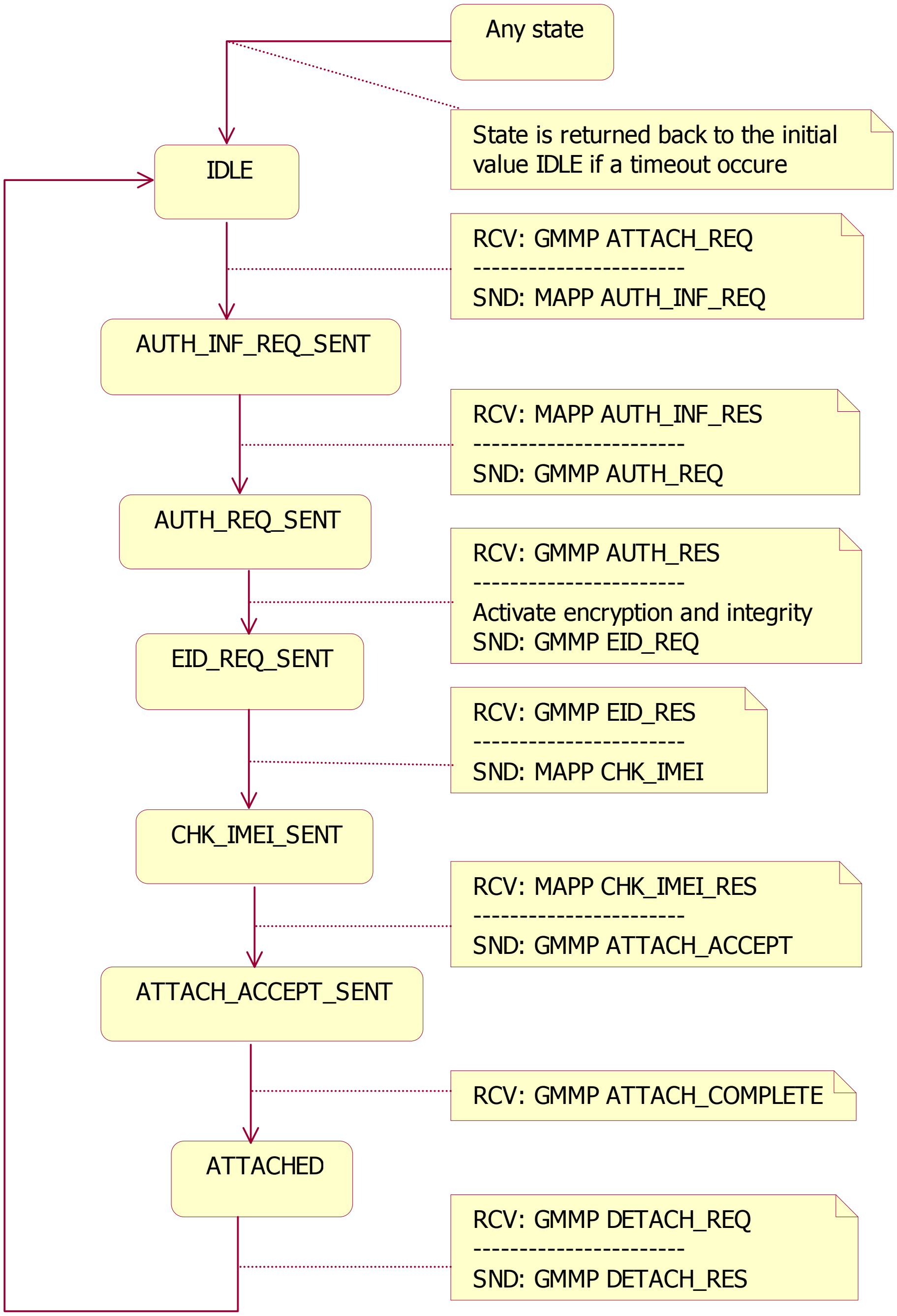


Figure 17 - SN state diagram

The initial state of SN is idle. As an ATTACH_REQ is received from UE and an AUTH_INF_REQ-message is sent to HE the state changes to AUTH_INF_REQ_SENT. The next expected step is to receive an AUTH_INF_RES from HE and to send an AUTH_REQ to UE. The state is then changed to AUTH_REQ_SENT. The AUTH_RES-message from UE contains a computed response. Encryption and integrity is switched on if this response correspond to the one supplied to SN from HE. On the other hand, if this fails, UE is informed that the authentication has been rejected. The attach procedure is cancelled and the entities returns to their initial state.

The arrival of an EID_RES-message, while in EID_REQ_SENT-state, triggers the dispatch of a CHK_IMEI-message to HE. The response on this message indicates whether the terminal id is found OK or not. If the terminal is not blacklisted an ATTACH_ACCEPT-message is sent to UE. When SN receives an ATTACH_COMPLETE from UE, SN reaches the state ATTACHED and the GMMP Attach procedure is finish. SN can receive a DETACH_REQ-message from UE. Such a message indicates that UE wish to detach from the network. A response is therefore sent and the SN-state returns to IDLE.

An important thing to be aware of, while dealing with signaling transport, is the possibility of timeouts. As shown in the state diagrams, timeouts trigger the cancellation of the procedure and return the entity back to its initial state. Timeout at UE will enforce a timeout at SN which in turn will result in that both entities return back to their initial states.

HE State

The functionality of HE can be narrowed down to request-response-processing. HE does not contain any state information since HE does initiate any actions it self. HE does however create and stores the authentication vector along with the cryptographic keys from the authentication procedure. These data are preserved and used during position checking until a new authentication request and a new authentication vector is generated. Hence, HE is not stateless even though no state machine is developed.

3.2.2.3 Call Control

Call Control (CC) is a collective term on messages used to setup and tare down a service. The messages in the CC protocol are listed in Table 5 below.

Table 5 - Call control messages

Message	Origin	End point	Comment
CALL_SETUP_REQ	UE	SN	Initiates the call setup procedure
CALL_SETUP_RES	SN	UE	Response indicating that the service is ready
CALL_SETUP_COMPLETE	UE	SN	UE confirms that it intends to use the service.
CALL_TERMINATE_REQ	UE	SN	UE wants to terminate the session.
CALL_TERMINATE_RES	SN	UE	SN responds that the service is ready to close.

The functionality that these messages provide will be shown in the following chapter describing the service setup.

3.2.2.3.1 Service Setup

A simple service is specified for demonstration purposes only. A simple echo-service was developed, as the service itself is not important. Messages sent from UE to SN are returned capitalized. Naturally UE has to be attached to SN in order for the service to be working. The call setup signaling sequence is shown in the following figure.

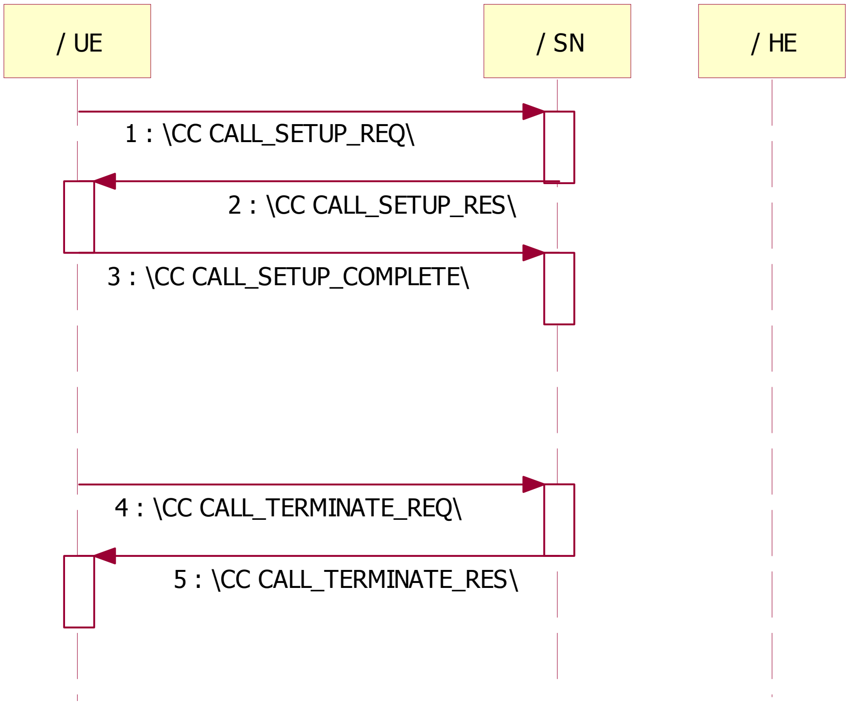

/ UE
/ SN
/ HE
1 : \CC CALL_SETUP_REQ\
2 : \CC CALL_SETUP_RES\
3 : \CC CALL_SETUP_COMPLETE\
4 : \CC CALL_TERMINATE_REQ\
5 : \CC CALL_TERMINATE_RES\

Figure 18 - Sequence diagram of service setup

A CALL_SETUP_REQ-message is sent to SN to initiate the service setup. This is a request for resources needed to use a specified service. The response from SN contains IP-address and port of the requested service. UE confirms to SN by sending CALL_SETUP_COMPLETE as the last message. The service is ready to use.

A CALL_TERMINATE_REQ is sent from UE to SN when UE is finish using the service. The arrival of such a message from UE initiates a teardown of the allocated resources. This makes it possible for SN to release unused resources.

3.2.2.3.2 Service State

State diagrams are used to visualize how the state of the service changes. The following diagrams provide a good insight in how the service state changes during the service setup-procedure.

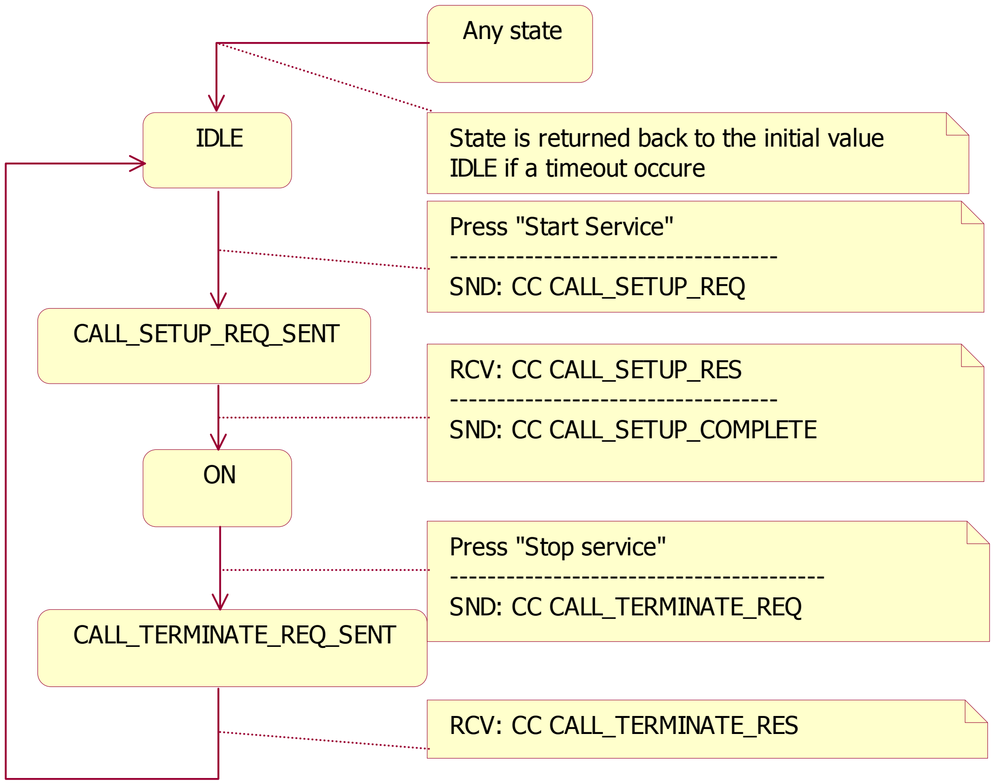


Figure 19 - Service state in UE point of view

Figure 19 shows how the UE service state changes as CALL_SETUP_REQ is sent to SN. CALL_SETUP_COMPLETE is sent at the arrival of CALL_SETUP_RES. The service state is ON and the service is ready to use. The UE service state changes to CALL_TERMINATE_REQ_SENT as terminate request is sent. The state returns to IDLE as the response is received from SN.

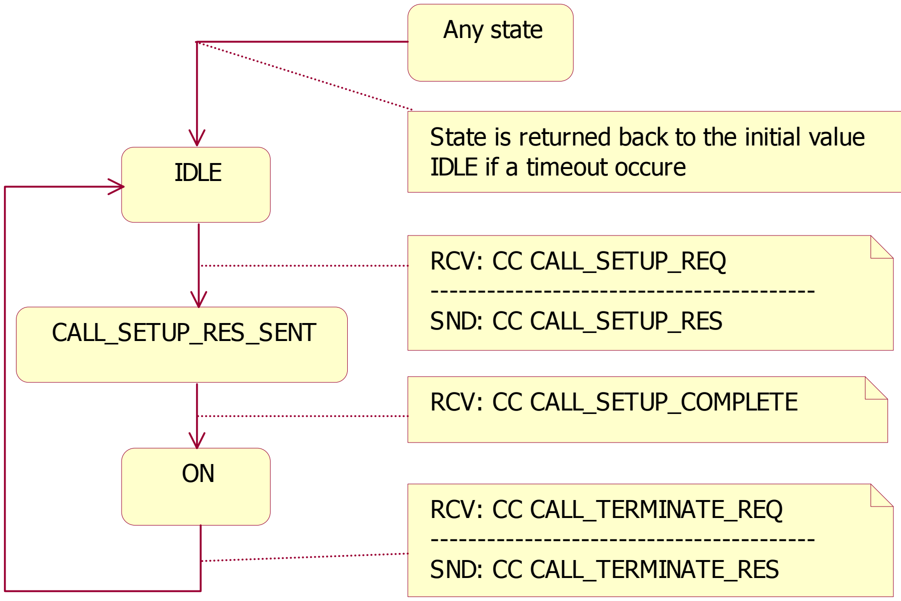


Figure 20 - Service state in SN point of view

Figure 20 shows how the SN service state changes as the call setup proceeds. The initial state is IDLE. It changes to CALL_SETUP_RES_SENT when CALL_SETUP_REQ is received by SN and its response is sent back to UE. The service is finally started as SN receives CALL_SETUP_COMPLETE from UE. SN receives a CALL_TERMINATE_REQ when UE wants to terminate the service connection. The SN service state returns to IDLE as the response is sent back to UE.

3.2.3 Applications

3.2.3.1 Introduction

Three entities, HE, SN and UE are needed in order to simulate a mobile environment. Each entity is represented by a standalone application. This way all processes can be ran distributed or on a single computer. The different applications are briefly described in the next sections.

3.2.3.2 Home Environment

The mobile operator's network in UMTS consists of a Home Location Register (HLR) and an Authentication Center (AuC). In the demonstrator this is simplified by merging it to one system called Home Environment (HE). HE contains a record of all its subscribers, including the crypto keys and IMSI. In this spatial system, HE also keeps a database of the Validity Areas (VA) associated with the user. In addition HE is given the role of keeping the EIR, which is a register that keeps track of stolen user equipments.

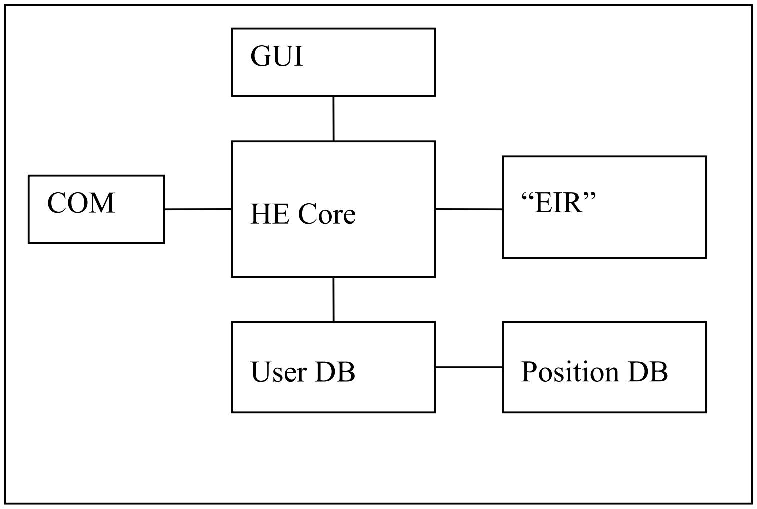


Figure 21 - Design Home Environment

Figure 21 shows the main design of HE. It consist of a core application with a graphical user interface (GUI) for auditing, a communication module for transporting the signaling messages between HE and SN, a user database for keeping the user data including the VA database, and finally HE also keeps the EIR.

The GUI mainly provides an auditory for test purposes. Besides that, HE runs by interacting with messages sent by SN. There is a preference window for making adjustments to the parameters MAX_USER_SPEED and MIN_LEAS_TIME (See chapter 2.7.2). The GUI can also save the auditory to file.

The communication module has a listening thread waiting for incoming messages from SN. The module also provides an interface to HE Core for sending messages to SN.

EIR keeps a record of different IMEI codes and their current status. The status may be white, grey or black.

The user database keeps the IMSI and the corresponding long-term pre-shared secret K. When HE is requested for authentication data, HE generates and stores an authentication vector. This consists of different crypto keys, an authentication token and a random seed used in the authentication procedure. On demand, this is sent to SN.

The position database provides a record of all the valid and invalid VA's associated with the user. This module will also perform the distance measurement between a given position and its nearest invalid area.

The HE core is the main module of the HE. This module is the one that handles incoming messages, performs the correct actions, and generates and sends a response back to SN.

3.2.3.3 Serving Network

In UMTS, the serving network consists of several nodes. All these nodes are in this demonstrator simplified as one called SN. SN provides the wireless access as well as the encryption and integrity protection over the air interface. SN performs parts of the authentication process on behalf of HE.

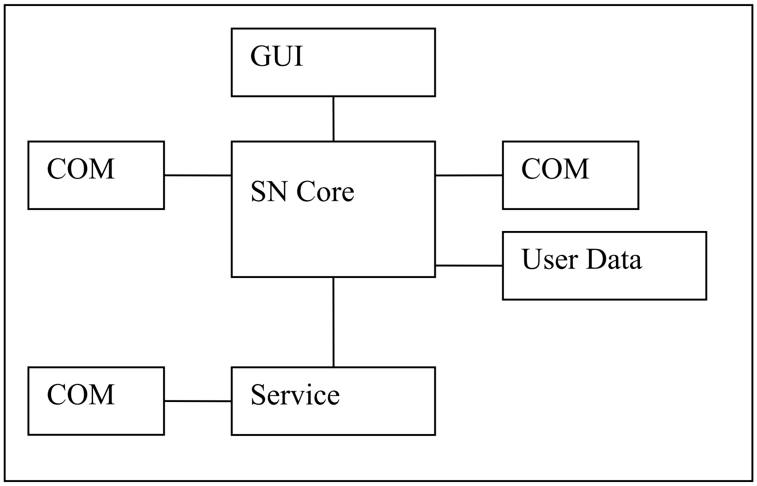


Figure 22 - Design Serving Network

The design of SN is shown in Figure 22. SN consists of two communication modules. One for communication with UE and one for communication with HE. Both communication modules take care of listening for incoming messages as well as providing an interface for sending messages.

After receiving a message, the SN Core handles the message according to the specification in chapter 3.2.2.

SN also provides a service for demonstration purposes. The service consists of a service module and a communication module. The communication module listens for incoming data and provides an interface for sending data back to UE. It is the SN Core that reserves the resources and takes down the service on demand from UE. The service module will read the incoming data from UE as ASCII, convert it to uppercase letters, and send it back to UE.

SN also has a module called User Data. This module keeps the IMSI and the authentication vector.

The GUI of SN provides an auditory of all activities in SN as well as all the state transitions. The auditory also keeps track of the amount of signaling data sent and received.

SN is designed to only serve one UE at a time. It is not in the scope of this demonstrator to serve more than one UE. There can also be initiated only one service at a time.

After the authentication procedure, all signaling between UE and SN is integrity protected using the integrity key found in the authentication vector received from HE. The user data sent through the service is always encrypted and integrity protected.

3.2.3.4 User Equipment

The User Equipment is a combination of mobile equipment, Location Measurement Unit and USIM (Universal Subscriber Identity Module).

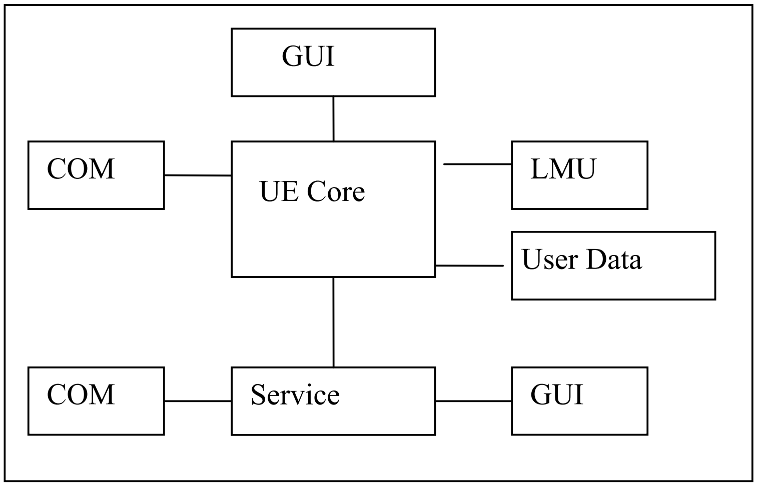


Figure 23 - Design User Equipment

The figure above describes the main design of UE. UE consist of a core with a GUI-front-end. The front-end present the functionality of UE, and an audit for data event logging. UE has one communication module. It provides an interface for sending messages in addition to handle incoming traffic. The UE Core takes proper action depending on the incoming message. The communication protocol and its state machines are described in chapter 3.2.2.

A location measurement unit (LMU) is implemented in order for UE to measure its position. UE Core communicates with LMU over a serial link.

UE has a service module. This module provides the possibility to use a service on the network. The service can send a text string to SN, which will respond with the same uppercased message. The service module has its own communication module, providing an interface for sending and receiving messages. The service module has its graphical front-end visualizing its functionality.

IMSI, IMEI, P-TMSI and keys are stored in a module called User Data. The keys are exchanged during the authentication procedure. One is used to integrity protect signaling between UE and SN. Another pair of keys makes it possible to encrypt and integrity protect all user data sent between HE and UE.

3.3 Implementation

3.3.1 Communication Protocols

3.3.1.1 Message Format

The communication protocols are implemented by defining message-build functions. These functions act as an interface providing an easy way to generate messages. The messages are based on the TLV (Type, Length, Value) format shown in the figure below.

Type	Length	Value

Figure 24 - TLV format

Messages build with this format is easy to process. The Type-field tells what kind of message it is. The length of the value field, in which the data is stored, is given in the Length-field.

3.3.1.2 Communication Ports

Communication between the different entities is directed to different ports. GMMP traffic sent from UE to SN is routed to port 3002 while SN is able to connect HE at port 3000. Response is, in both cases, returned to the origin port. The ECHO service at SN is served at a dynamic port assigned during service setup.

3.3.1.3 Protocol Stack

The protocols defined in 3.2.2 interact with each other and forms the protocol stack showed below. UE communicates with the GPS using Garmin text format over a serial link. The position data is transported transparent over SN from UE to HE using HCP. Other messages sent between UE and SN uses GMMP or CCP over UDP/IP. Communication between SN and HE is performed with MAPP over UDP/IP.

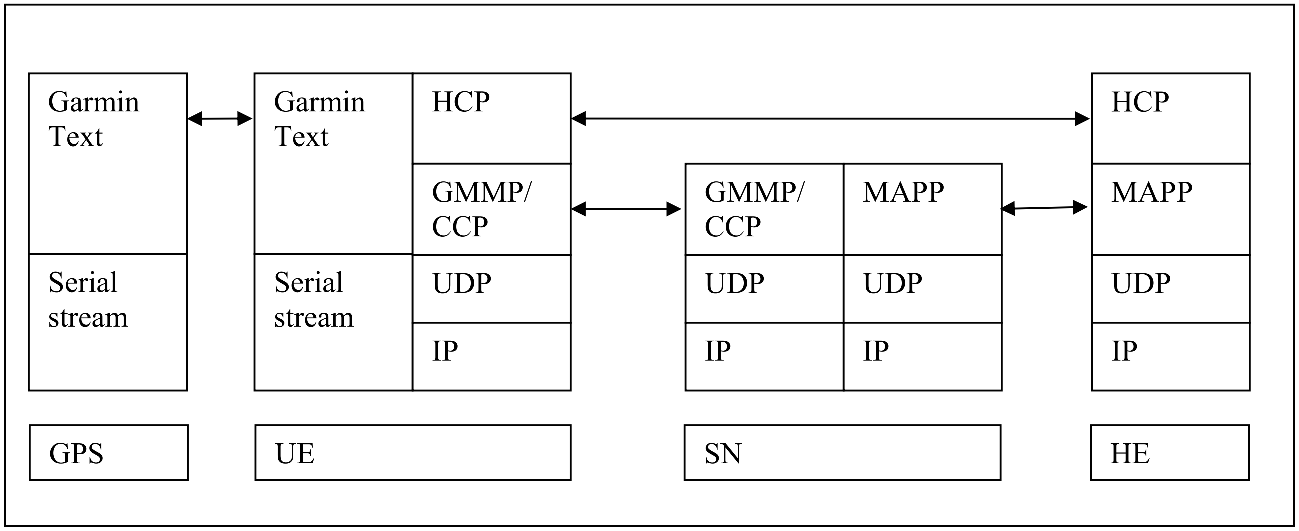
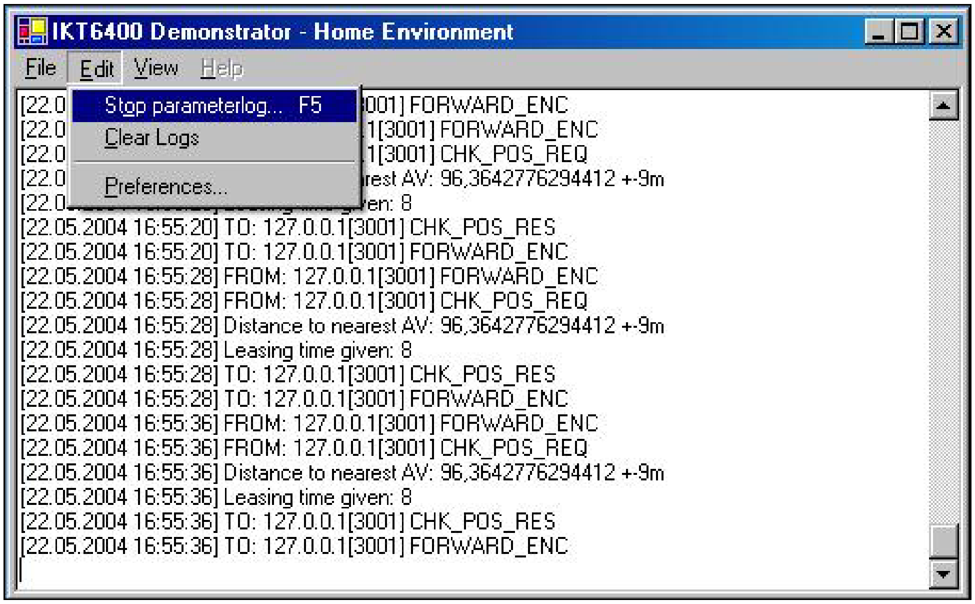


Figure 25 - Protocol Stack

3.3.2 Home Environment

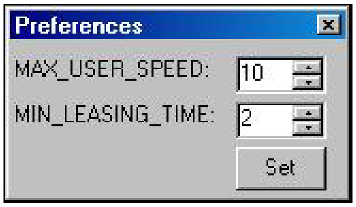
3.3.2.1 Graphical User Interface



```
[22.0                          001] FORWARD_ENC
[22.0                          1[3001] FORWARD_ENC
[22.0                          1[3001] CHK_POS_REQ
[22.0                          rest AV: 96,3642776294412 +-9m
[22.0                          ven: 8
[22.05.2004 16:55:20] TO: 127.0.0.1[3001] CHK_POS_RES
[22.05.2004 16:55:20] TO: 127.0.0.1[3001] FORWARD_ENC
[22.05.2004 16:55:28] FROM: 127.0.0.1[3001] FORWARD_ENC
[22.05.2004 16:55:28] FROM: 127.0.0.1[3001] CHK_POS_REQ
[22.05.2004 16:55:28] Distance to nearest AV: 96,3642776294412 +-9m
[22.05.2004 16:55:28] Leasing time given: 8
[22.05.2004 16:55:28] TO: 127.0.0.1[3001] CHK_POS_RES
[22.05.2004 16:55:28] TO: 127.0.0.1[3001] FORWARD_ENC
[22.05.2004 16:55:36] FROM: 127.0.0.1[3001] FORWARD_ENC
[22.05.2004 16:55:36] FROM: 127.0.0.1[3001] CHK_POS_REQ
[22.05.2004 16:55:36] Distance to nearest AV: 96,3642776294412 +-9m
[22.05.2004 16:55:36] Leasing time given: 8
[22.05.2004 16:55:36] TO: 127.0.0.1[3001] CHK_POS_RES
[22.05.2004 16:55:36] TO: 127.0.0.1[3001] FORWARD_ENC
```

Figure 26 - HE GUI

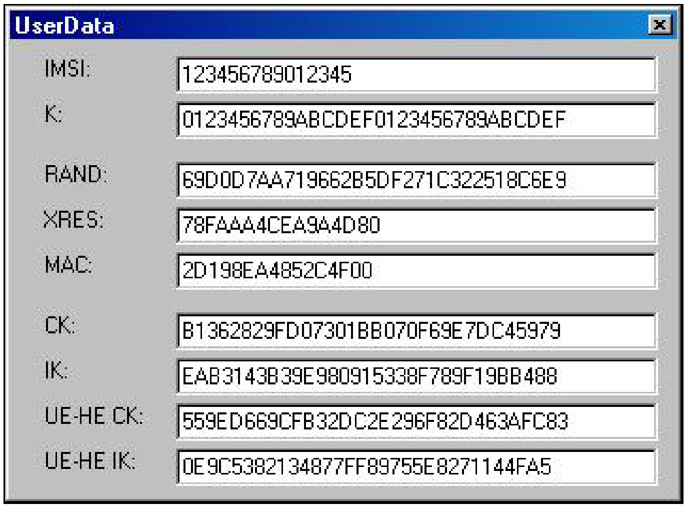
The main window of HE's GUI is an auditory of messages and position checking. There is a main menu for starting and stopping the HE and for handling the auditory. It is also possible to save the auditory to file. The auditory consist of a message log, and a parameter log. The message-log is what is seen in Figure 26. The parameter log produces a semicolon separated file used during the parameter testing in chapter 4.



MAX_USER_SPEED: 10
MIN_LEASING_TIME: 2

Figure 27 - HE Preferences

Besides the main window, the GUI offers the possibility to change the parameters used in HE. It is also possible to view the IMSI and the authentication vector associated with the user.



IMSI: 123456789012345
K: 0123456789ABCDEF0123456789ABCDEF
RAND: 69D0D7AA719662B5DF271C322518C6E9
XRES: 78FAAA4CEA9A4D80
MAC: 2D198EA4852C4F00
CK: B1362829FD07301BB070F69E7DC45979
IK: EAB3143B39E980915338F789F19BB488
UE-HE CK: 559ED669CFB32DC2E296F82D463AFC83
UE-HE IK: 0E9C5382134877FF89755E8271144FA5

Figure 28 - HE User data

3.3.2.2 Communication module

The communication between SN and HE is performed using the signaling protocol MAPP (See chapter 3.2.2.2.2). This protocol is transported by UDP over IP. The communication module has a thread constantly listening for incoming messages on the known UDP port 3000. Any incoming messages are de-serialized and sent to the HE Core for further handling. The communication module also provides a Send – method for transmission of MAPP messages. All incoming and outgoing messages are audited.

3.3.2.3 User data

The User Data module keeps all the information on the subscriber. It consists of the IMSI, the pre-shared secret K and all the authentication and crypto keys needed. E.g. it holds the authentication vector to send to SN on demand. It also generates the crypto key UE-HE CK and UE-HE IK used for encryption and integrity protection of the position message sent from UE to HE. The key is generated in the same way as CK and IK with the difference that the input key K is X-OR'd with the IMSI. The IMSI is repeated to fill the correct amount of bytes used in K. HE supports storing user data for multiple subscriptions. In the demonstrator, only data of one pre-recorded user is stored. The data of this user is as follows:

IMSI:	123456789012345
K:	0123456789ABCDEF0123456789ABCDEF

3.3.2.4 EIR

The attach procedure also check the serial number of the mobile terminal. For simplicity, this is implemented in HE. On demand, HE checks the IMEI against the register stored in EIR. The pre-recorded data is:

IMEI:	123456789012345,	123456789012346,	123456789012347
STATUS:	WHITE,	GREY,	BLACK'

The IMEI used in the UE is 12345679012345. For testing of different IMEI-status, the UE may try using some of the other IMEIs listed above.

3.3.2.5 Position DB

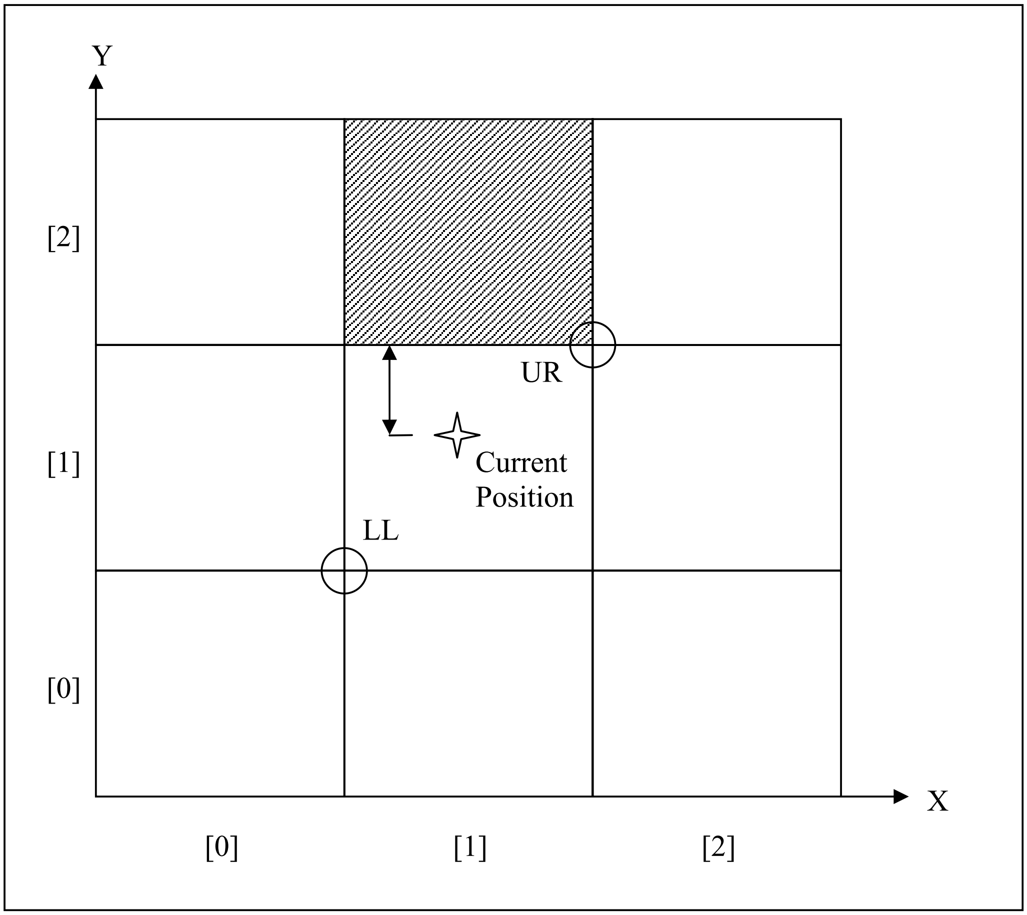


Figure 29 - Grid of Validity Areas

The position database holds the information on the VA associated with the subscriber. The database is represented by a two-dimensional array of rectangle-shaped Areas. Each Area is represented by a lower-left point (LL) and an upper-right point (UR). An Area also has info of the validity of that rectangle. The points are represented by 64 bit signed values for X and Y. The value is calculated by converting longitude and latitude to degrees. Longitude and latitude are written on the form DDD°MM.mmmm'. E.g. N 008°22.395' which reads 8 degrees, 22.395 minutes north. The position is converted to degrees by using formula [V]. Longitude is used for X, and latitude is used for Y.

$$[V] \qquad \mathit{Degrees} = \mathit{DDD} + (\mathit{MM.mmmm} / 60)$$

The Position DB module provides a public method called CheckPos. This method takes position as argument. First it finds the area in which the position lays by using a linear search algorithm. Then it checks all the adjacent areas. It calculates the shortest distance to the nearest area of opposite validity. If in a valid area, this distance is positive. If in an invalid area, the distance is returned negative. If there are no adjacent cells with opposite validity, the distance is measured as the distance to the nearest neighbor + the width of the neighbor. The GetDistance – method used in this algorithm, takes the position and the nearest neighbor as arguments. A Boolean argument indicating whether to include the width of the neighbor in the distance measuring is also provided. The distance is calculated according to formula [I].

```
public double CheckPos(GPS.TPV pos, string IMSI)
{
[…] // Some init code left out
// Find X column
//     Using linear search. More efficient with large arrays
//     to use binary search or some other algorithm.
for(i = 0; i < gridsize; i++)
{
       if((grid[i,0].Left < p.X) && (grid[i,0].Right >= p.X))
       {
              // Find Y element
              for(j = 0; j < gridsize; j++)
              {
              if((grid[i,j].Top >= p.Y) && (grid[i,j].Bottom < p.Y))
                     break;
              }
              break;
       }
}

// Found the area where the position is within
if((i < gridsize) && (j < gridsize))
{
// Not all grids have 8 possible neighbours.
// Check if the x is at an edge
int iOffStart = (i == 0) ? 0 : -1;
int iOffStop = (i < (gridsize - 1)) ? 1 : 0;
int jOffStart = (j > 0) ? -1 : 0;
int jOffStop = (j < (gridsize - 1)) ? 1 : 0;

// Seach linearly through the neighbours
// Save the shortest distance found.
for(int iOff = iOffStart; iOff <= iOffStop; iOff++)
{
for(int jOff = jOffStart; jOff <= jOffStop; jOff++)
{
       if((iOff == 0) && (jOff == 0))
       {
              //Skip, this is the one you're in
       }
       else if(grid[i+iOff, j+jOff].Valid != grid[i,j].Valid)
       {
              Opposite_found = true;
              // Measure distance to neighbours
              // with opposite validity
              double temp = GetDistance(p, grid[i + iOff, j + jOff], iOff, jOff, false);
              // Store the shortest distance
              if(temp < distance)
                     distance = temp;
       }
       else
       {
              // Measure distance to neighbours
              // with same validity
              double temp = GetDistance(p, grid[i + iOff, j + jOff], iOff, jOff, true);
              // Store the shortest distance
              if(temp < distance_same_validity)
                     distance_same_validity = temp;
       }
}
}
}

// Return distance, positive if in valid area, else negative
ret = Opposite_found ? distance : distance_same_validity;
return ret * ((i < gridsize) && (j < gridsize) && (grid[i,j].Valid) ? 1 : -1);
}
```

3.3.2.6 HE Core

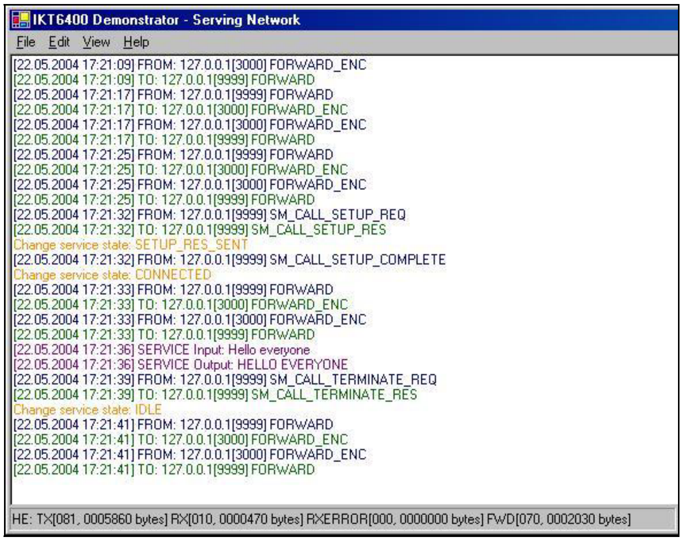
The core module handles all the incoming messages according to Table 6. If the message is not recognized, it is silently discarded. If the integrity check fails, an entry is made in the auditory, and the message is silently discarded. HE maintains no state machine.

Table 6 - HE Core message handling

SND_AUTH_INF	Checks the user database for the IMSI, and returns the AV generated for that subscription
CHK_IMEI	Checks the EIR for the IMEI, and returns the status for that user equipment.
FORWARD_ENC	This message is originated at UE. The payload is encrypted and integrity protected. When getting this message, HE checks the payload integrity and decrypts it. Then it deserializes the payload. In this demonstrator, the only message type being carried within a FORWARD_ENC message, is the CHK_POS_REQ.
CHK_POS_REQ	HE gets the VA information, calculates a leasing time, and returns a confidentiality and integrity protected CHK_POS_RES message containing the leasing time.

3.3.3 Serving Network

3.3.3.1 Graphical User Interface

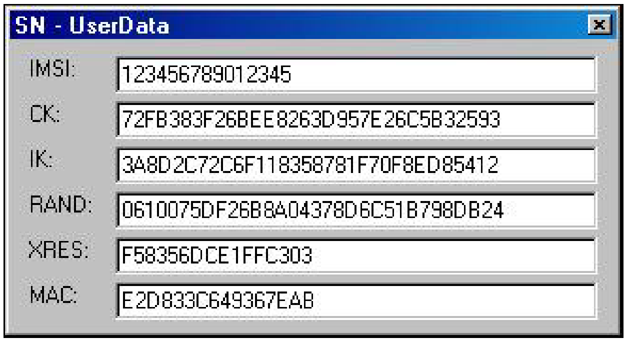


```
[22.05.2004 17:21:09] FROM: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:09] TO: 127.0.0.1[9999] FORWARD
[22.05.2004 17:21:17] FROM: 127.0.0.1[9999] FORWARD
[22.05.2004 17:21:17] TO: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:17] FROM: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:17] TO: 127.0.0.1[9999] FORWARD
[22.05.2004 17:21:25] FROM: 127.0.0.1[9999] FORWARD
[22.05.2004 17:21:25] TO: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:25] FROM: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:25] TO: 127.0.0.1[9999] FORWARD
[22.05.2004 17:21:32] FROM: 127.0.0.1[9999] SM_CALL_SETUP_REQ
[22.05.2004 17:21:32] TO: 127.0.0.1[9999] SM_CALL_SETUP_RES
Change service state: SETUP_RES_SENT
[22.05.2004 17:21:32] FROM: 127.0.0.1[9999] SM_CALL_SETUP_COMPLETE
Change service state: CONNECTED
[22.05.2004 17:21:33] FROM: 127.0.0.1[9999] FORWARD
[22.05.2004 17:21:33] TO: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:33] FROM: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:33] TO: 127.0.0.1[9999] FORWARD
[22.05.2004 17:21:36] SERVICE Input: Hello everyone
[22.05.2004 17:21:36] SERVICE Output: HELLO EVERYONE
[22.05.2004 17:21:39] FROM: 127.0.0.1[9999] SM_CALL_TERMINATE_REQ
[22.05.2004 17:21:39] TO: 127.0.0.1[9999] SM_CALL_TERMINATE_RES
Change service state: IDLE
[22.05.2004 17:21:41] FROM: 127.0.0.1[9999] FORWARD
[22.05.2004 17:21:41] TO: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:41] FROM: 127.0.0.1[3000] FORWARD_ENC
[22.05.2004 17:21:41] TO: 127.0.0.1[9999] FORWARD

HE: TX[081, 0005860 bytes] RX[010, 0000470 bytes] RXERROR[000, 0000000 bytes] FWD[070, 0002030 bytes]
```

Figure 30 - SN Graphical User Interface

Figure 30 shows the GUI in SN. The main window contains the auditory of all messages and state transitions. The status bar keeps track of the amount of messages and bytes sent to and from HE and UE[1]. The audit can be saved to file, and will be stored as Rich Text Format.



IMSI: 123456789012345

CK: 72FB383F26BEE8263D957E26C5B32593

IK: 3A8D2C72C6F118358781F70F8ED85412

RAND: 0610075DF26B8A04378D6C51B798DB24

XRES: F58356DCE1FFC303

MAC: E2D833C649367EAB

Figure 31 - SN User data

The GUI also presents the user data temporary stored for the ongoing user session.

3.3.3.2 Communication modules

SN has several communication modules. The one to be presented here are the two modules taking care of signaling between UE and SN, and the one for signaling between SN and HE. Both modules are designed around the same idea of having one thread listening for incoming messages, as well as providing an interface for sending response messages. The module communicating with HE handles reception and sending of MAPP messages. The messages are transported by UDP over IP on the known port 3001. The one communicating with UE handles reception and sending of GMMP and CCP messages. The messages are transported by UDP over IP on the known UDP port 3002. Depending on whether integrity is switched on or not, the messages received by UE is checked for integrity. If integrity check fails, an entry is made in the auditory, and the message is silently discarded. On sending messages, integrity protection is added dependant on whether integrity is switched on or not. For more details on when integrity check is on, see chapter 3.2.2.2.3.

3.3.3.3 User Data

During the AKA procedure, SN asks HE for the authentication vector of the current user. This AV is stored along with the IMSI of the user. The AV contains e.g. CK, IK, RAND, XRES and MAC.

3.3.3.4 SN Core

SN keeps a state machine for each session according to chapter 3.2.2.2.5. The SN Core is the one handling incoming messages. After receiving a message from UE, SN handles the message according to which state the state machine holds. A timer thread is started when SN is sending out a request message and expecting a response. If the timer fires because of a lost or delayed response message, SN is brought to the correct state according to the specification of the state machine. If the message arrives late, it will be handled according to the state the SN is in. Any messages received out of scope are silently discarded.

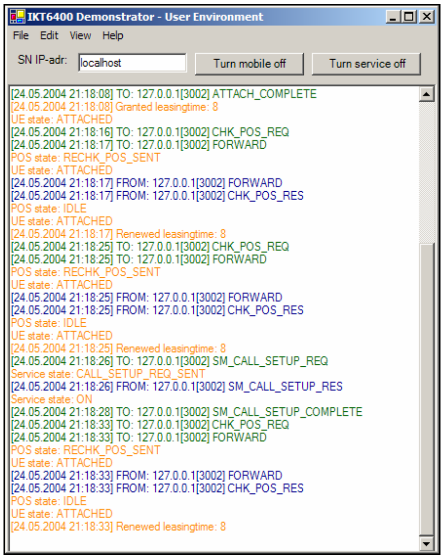
[1] The figure is cut to fit. Only signaling traffic between HE and SN is visible.

3.3.3.5 Service

The service is implemented using a TCP connection on a dynamically provided port. The port number is given to UE during call setup signaling. The data in the service are encrypted and integrity protected. A message is recognized by the use of the trailing carriage return (CR) followed by the line feed (LF). CR has the value ‘\r’ or hexadecimal 0x13 and LF has the value ‘\n’ or 0x0A hex.

3.3.4 User Equipment

3.3.4.1 Graphical User Interface

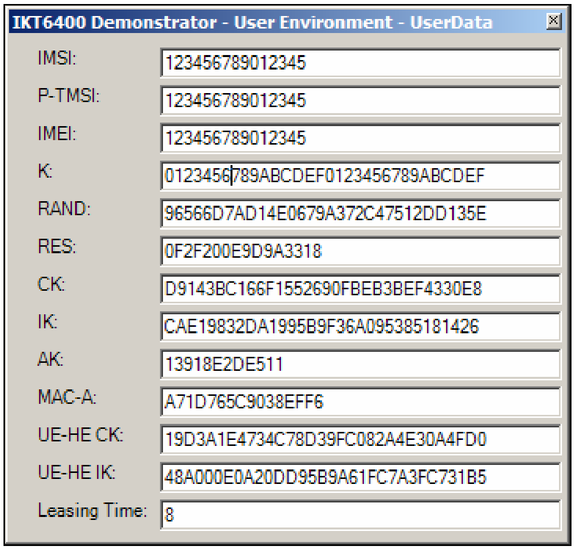


SN IP-adr: localhost

```
[24.05.2004 21:18:08] TO: 127.0.0.1[3002] ATTACH_COMPLETE
[24.05.2004 21:18:08] Granted leasingtime: 8
UE state: ATTACHED
[24.05.2004 21:18:16] TO: 127.0.0.1[3002] CHK_POS_REQ
[24.05.2004 21:18:17] TO: 127.0.0.1[3002] FORWARD
POS state: RECHK_POS_SENT
UE state: ATTACHED
[24.05.2004 21:18:17] FROM: 127.0.0.1[3002] FORWARD
[24.05.2004 21:18:17] FROM: 127.0.0.1[3002] CHK_POS_RES
POS state: IDLE
UE state: ATTACHED
[24.05.2004 21:18:17] Renewed leasingtime: 8
[24.05.2004 21:18:25] TO: 127.0.0.1[3002] CHK_POS_REQ
[24.05.2004 21:18:25] TO: 127.0.0.1[3002] FORWARD
POS state: RECHK_POS_SENT
UE state: ATTACHED
[24.05.2004 21:18:25] FROM: 127.0.0.1[3002] FORWARD
[24.05.2004 21:18:25] FROM: 127.0.0.1[3002] CHK_POS_RES
POS state: IDLE
UE state: ATTACHED
[24.05.2004 21:18:25] Renewed leasingtime: 8
[24.05.2004 21:18:26] TO: 127.0.0.1[3002] SM_CALL_SETUP_REQ
Service state: CALL_SETUP_REQ_SENT
[24.05.2004 21:18:26] FROM: 127.0.0.1[3002] SM_CALL_SETUP_RES
Service state: ON
[24.05.2004 21:18:28] TO: 127.0.0.1[3002] SM_CALL_SETUP_COMPLETE
[24.05.2004 21:18:33] TO: 127.0.0.1[3002] CHK_POS_REQ
[24.05.2004 21:18:33] TO: 127.0.0.1[3002] FORWARD
POS state: RECHK_POS_SENT
UE state: ATTACHED
[24.05.2004 21:18:33] FROM: 127.0.0.1[3002] FORWARD
[24.05.2004 21:18:33] FROM: 127.0.0.1[3002] CHK_POS_RES
POS state: IDLE
UE state: ATTACHED
[24.05.2004 21:18:33] Renewed leasingtime: 8
```

Figure 32 - UE Graphical User Interface

The GUI of UE is illustrated in the figure above. The main window contains an auditory showing all messages sent and received together with a text field and two buttons. The text field is used to alter the destination address of SN during pre-testing. The two buttons makes it possible to turn the mobile terminal and service on and off. It is possible to save the audit to file in Rich Text Format.



IMSI:	123456789012345
P-TMSI:	123456789012345
IMEI:	123456789012345
K:	0123456789ABCDEF0123456789ABCDEF
RAND:	96566D7AD14E0679A372C47512DD135E
RES:	0F2F200E9D9A3318
CK:	D9143BC166F1552690FBEB3BEF4330E8
IK:	CAE19832DA1995B9F36A095385181426
AK:	13918E2DE511
MAC-A:	A71D765C9038EFF6
UE-HE CK:	19D3A1E4734C78D39FC082A4E30A4FD0
UE-HE IK:	48A000E0A20DD95B9A61FC7A3FC731B5
Leasing Time:	8

Figure 33 - UE User data

Figure 33 shows that it is possible to view the different values assigned for the current session.

3.3.4.2 Communication modules

The communication module attached to UE Core handles all signaling sent from and received by UE. The module is designed around the same idea of having one thread listening for incoming requests. In addition it provides an interface for sending signaling messages. Communication between UE and SN is handled by GMMP and is transported by UDP over IP. If integrity is switched on, all incoming messages are checked for integrity, while integrity is added on sending. Incoming messages is discarded if integrity check fails, in addition a note in the audit.

3.3.4.3 User data

Keys and identities are exchanged during the authentication procedure. All of these are stored in the User Date module. The graphical view of values stored in User Data in given in Figure 33. IMSI, IMEI and K are predetermined values, specific to each instance of UE. All the other values are generated and exchanged through the authentication procedure. Time to next position check, given in seconds, is stored in the value "Leasing time".

3.3.4.4 Location Measurement Unit

The LMU module handles the position measurement. The GPS report current position each second. The LMU module reads this information from the GPS over a serial link. The position is then sent to HE for verification. HE responds with a leasing time if the position is found valid. The position is checked over and over again. The interval between them is decided by the granted leasing time.
The position exchange is sent transparently from UE to HE and back with help from SN.
UE-HE CK and UE-HE IK encrypt and integrity protects all signaling messages to secure an uninterrupted dispatch between HE and UE.

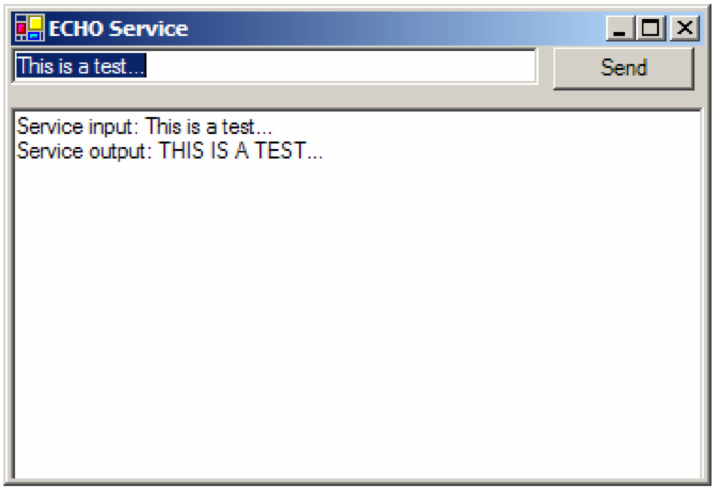
3.3.4.5 UE Core

The UE Core module makes the other modules work together. It serves as a connection between them. As a message is received by the communication module it is processed. Response is composed and sent in reply. The UE Core keeps a state machine for the session according to chapter 3.2.2.2.5. In addition it keeps track of the service state machine.

UE Core is responsible for handling timeouts. Signaling transported by UDP over IP may be interrupted and disappear. The application would dead lock without timeouts. Timeouts is therefore implemented to make the application tolerant to loss of signaling messages. In case of timeouts, the application is returned to its prior state as described in 3.2.2.2.5.

3.3.4.6 Service

The Service module implements a service in UE. The service shows that it is possible for UE and SN to interact while using information provided in the authentication procedure. The Service has a separate communication module. This module receives and sends messages related to the service offered by SN. All service messages sent between SN and UE are integrity protected.



This is a test...

Service input: This is a test...
Service output: THIS IS A TEST...

Figure 34 – UE Service Graphical User Interface

It is a simple echo service. When pushing the Send button, the message in the text field is sent to SN. The message will be returned by SN uppercased.

3.3.5 Security algorithms

[3GPP TS 33.105] specifies several security algorithms used for producing keys and for confidentiality and integrity protection

Table 7 - UMTS security algorithms [Køien, 2004]

Algorithm	Purpose/usage	O – operator specific S – Fully standardized	Location
f0	Random challenge generating function	O	AuC
f1	Network authentication function	O - (MILENAGE)	USIM and AuC
f1*	Re-synchronization message authentication function	O - (MILENAGE)	
f2	User challenge-response authentication function	O - (MILENAGE)	
f3	Cipher key derivation function	O - (MILENAGE)	
f4	Integrity key derivation function	O - (MILENAGE)	
f5	Anonymity key derivation function for normal operation	O - (MILENAGE)	
f5*	Anonymity key derivation function for re-synchronization	O - (MILENAGE)	
f6	MAP encryption algorithm	S	MAP nodes
f7	MAP integrity algorithm	S	
f8	UMTS encryption algorithm	S – (KASUMI)	MS and RNC
f9	UMTS integrity algorithm	S – (KASUMI)	

This demonstrator uses the Milenage Algorithm set [3GPP TS 35.206] for the cryptographic functions (f1-f5*). Kasumi is used for f8 and f9. For f0, the cryptographic strong random function RNGCryptoServiceProvider provided by the .NET framework is used [MSDN]. Milenage is ported from ANSI C to C# using the example sets in [3GPP TS 35.206]. f8 and f9, including Kasumi is ported from ANSI C to C# using [3GPP TS 35.201] and [3GPP TS 35.202]. The main issues in porting from ANSI C to C# is the use of pointers. This was solved by using arrays and array-indexes.

Some simplifications are made to the use of the security algorithms. When using f8, the count, bearer and direction data are simply set to zero. This will decrease the security, but for the use in this demonstrator, the simplification will not affect the security significantly. Also the integrity function f9 has a count, a fresh and a direction argument which all were set to zero.

3.4 Testing

3.4.1 Introduction

The testing was done module by module. After each module had passed the testing, the applications were tested together with the other applications for integrity validation.

3.4.2 Security algorithms

The security algorithms were tested using 3GPP test documents. Milenage was tested using [3GPP TS 35.207] and [3GPP TS 35.208]. Kasumi, f8 and f9 were tested using [3GPP TS 35.203] and [3GPP TS 25.204]. All tests were successfully completed.

3.4.3 HE

3.4.3.1 COM

COM shall be able to receive messages from SN on UDP port 3000. To test this, a test program is written. The test program is capable of sending messages over UDP to a given IP-address and UDP-port. By using the debugging feature of Visual Studio .NET, it is possible to stop the code on receiving data. It is also possible to see the values of variables during runtime. The module was tested by creating a message with the build-methods in MAPP. This message was serialized with the serialize-method. The message was sent to the correct IP-address to UDP port 3000 and correctly transferred and read by the COM module. The message was de-serialized back to a MAP message. The contents of the original and the transferred message were identical.

The COM module also provides a send method which is implicitly tested during the above test.

3.4.3.2 EIR

EIR is a simple record of the pairs IMEI and terminal status. The status can be WHITE, GREY or BLACK. If the IMEI is found, the terminal status is sent to SN. The value NOT_AVAILABLE is sent when the IMEI is not found. This module is tested by sending using the different stored values of IMEI (see the implementation chapter) and one that is not stored. The testing of the EIR module was successfully completed.

3.4.3.3 GUI

Starting and stopping of HE was tested. The function starts or stops the COM module. This worked fine. The log-window worked fine. The saving of logs also worked fine. The preferences window giving the possibility to change some parameters during runtime was tested by debugging the application in runtime. It worked as it should. The viewing of user data was tested. The data changed correctly according to the specifications.

3.4.3.4 Position DB

This database contains the validity areas associated with the user. The module offers a method called CheckPos. It returns the distance from the current position, to the nearest area of opposite validity. The coordinates of a test-area was entered in the database. The method was tested by entering different pre-chosen positions which were verified using a map-program. The algorithm was tested with different validity of the current VA, and with the nearest VA with opposite validity being in every direction of the current VA. The testing of the module was completed successfully.

3.4.3.5 HE Core

The core handles incoming messages from SN. The last generated keys and authentication vector is stored in the user database. The module is tested by simulating messages without using the COM modules. The debugging process allows monitoring that the state machine behaves according to the specification. The module was tested successfully for all message types.

3.4.4 SN

3.4.4.1 GUI

The graphical interface consists of an auditory, a status bar and a user data form. The status bar is updated correctly for every incoming and outgoing message. The user data is updated correctly whenever new data is collected from HE.

3.4.4.2 COM

The communication module shall be able to receive messages and send messages. One module is for communication with UE, and the other is for communication with HE. In addition to sending and receiving, the UE COM module takes care of integrity protection. The module was tested with and without integrity protection turned on. It was also tested with integrity deliberately erroneous. Both COM modules were tested successfully.

3.4.4.3 User Data

The user data was stored and updated correctly.

3.4.4.4 SN Core

The core handles incoming messages, and maintains a state machine. This module was tested by simulating messages without going through the COM modules. No timeouts were used during testing. This allows running a debugging process without having the timers go off prematurely.

The test of the state machine was done with a complete system test using all applications. The logs monitor the state machine and it is easy to see that it behaves according to protocol. The module was tested and found working according to chapter 3.2.2.2.5.

The use of timeout was tested successfully after the other tests were completed ok.

3.4.4.5 Service

This module was tested along with the integration test, and worked as intended.

3.4.5 UE

3.4.5.1 LMU

The LMU module shall supply the application with information regarding the position. The module communicates with a GPS using a serial link. The GPS reports the position every second. The LMU module is tested and found to return valid position information.

3.4.5.2 COM

UE has a communication module for interaction with SN. This module is capable of sending and receiving messages from SN on UDP port 9999. A test application was used in order to fully test the functionality of COM. The application is able to generate and send every message that UE can receive (see 0). Incoming messages were checked using the debug feature in the IDE. Messages were generated and serialized using functions in the GMPP protocol before sent to the COM module. Messages were de-serialized as they were received by COM. After de-serialization, parameters inside the message were checked to match those sent. They matched.

3.4.5.3 User data

User data is a register that keeps track of stored and exchanged values. Values stored at UE, SN and HE were compared to verify that the module worked as it was intended to. Values stored in the User data module is exchanged and used during the authentication procedure. Figure 33 visualize the User data.

3.4.5.4 GUI

The GUI presents the functionality of UE. The GUI has an audit, address input field, and two buttons. The audit is an event log. Events like incoming / outgoing messages and state transitions are shown here. The buttons make it possible to turn the mobile terminal and service on and off. Testing the GUI module revealed some interaction problems among the different modules that were fixed. A few problems regarding writing to the audit were corrected. Some adjustments were made to assure that it was not possible to start the service when the mobile terminal was switched off. The opportunity to save logs was tested and verified.

3.4.5.5 Service

UE has a service module. The module makes it possible to connect to and use a service provided by SN. The Service module consists of a smaller COM module and a GUI. The graphical front-end makes it possible to type a message and send it to SN. The response from SN is shown in a text window. The COM module handles sending when the Send button is pressed. Incoming messages are processed by the same COM module and written to the text window. Minor adjustment had to be done to support the Norwegian letters æ, ø and å.

3.4.5.6 UE Core

UE Core is the link between all the other modules. UE Core takes proper action as COM receive incoming messages. It handles the state machines of the service and the mobile terminal. The debug option and the auditory provided by GUI is used to check the behavior of the states machines. The states machines are described in section 3.2.2.2.5. Timers are implemented to assure that the application will not deadlock in case of signaling loss. A timer is started when a request is sent to SN and stopped when response is received. UE is brought back to its correct state if the timer is not stopped within a certain time. Another timer assures that the position is rechecked every time the leasing time is elapsed. This is done to be sure of the validity of the current position. UE Core was successfully tested.

4 Results

4.1 Testing the parameters

4.1.1 Test Setup

For testing purposes we defined two areas using GPS coordinates. One area was defined as valid, another as invalid (See Figure 35). A road was going approximately north-south through the boundaries of the areas. This road was used during testing. A WLAN access point was situated a little south of the test site for communication between UE and SN. The tests were done iteratively by first testing small fractions of the thesis, and them putting them together to form an entirely working system.

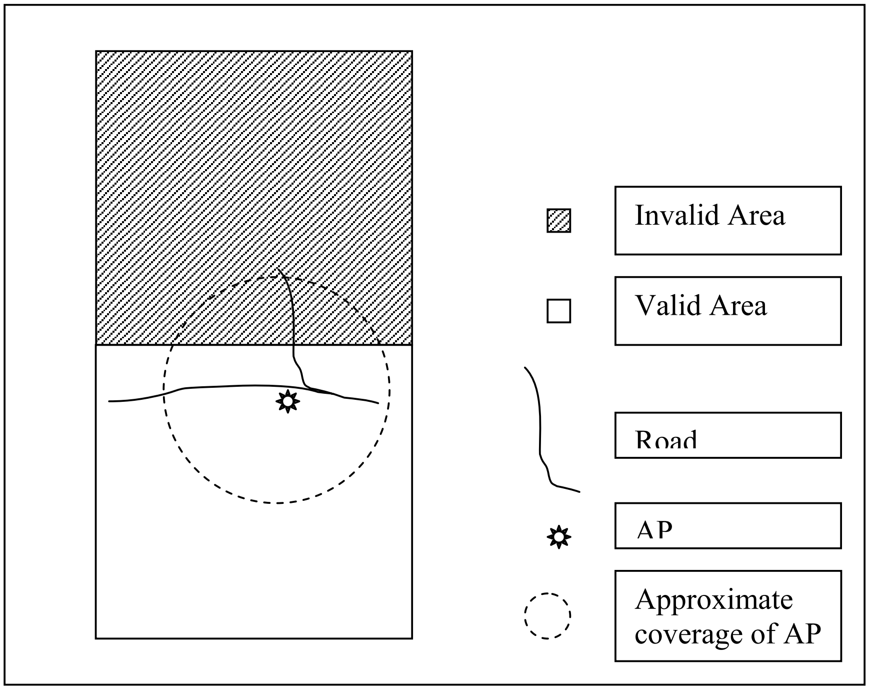


Figure 35 - Test area

The different applications audit the different parameters during testing according to Table 8.

Table 8 - Auditory

Audit	Description	Application
Position measurement	Time, Velocity, Position	UE, HE
Area-data	Validity of current rectangle	HE
Authentication state	Authenticated, not authenticated, timestamp	UE
Distance to nearest negative VA	In meters	HE
Given leasing time	In seconds	UE, HE

4.1.2 Always inside

This test shall investigate the system behavior when a user moves around entirely inside of a zone 3 (see chapter 2.7.2.3). The user shall at all times be within the boundaries of a positive VA, and never closer to the boundaries than formula [II] says. The reason for this is that the user can be locked out if moving within zone 2.

The test is executed over a short period of time. The audit must record both occasions when the user is standing still and while the user is moving.

4.1.3 Always outside

This test shall investigate the system behavior when a user moves around entirely inside of a negative validation area. The user shall at all times be within the boundaries of a negative VA, and never crossing the boundaries.

The test is executed over a short period of time. The audit must record both occasions when the user is standing still and while the user is moving.

4.1.4 Crossing boundary

This test shall investigate the systems behavior when a user moves across the boundaries of different zones. There are two tests, one for each direction of moving between zone 1 and zone 3.

A: (z1→z3)
Start inside a positive VA. Walk toward the boundary of a negative VA in a constant speed. Measure the distance to the boarder at the time the user is denied access. Repeat 5 times for each speed and calculate the mean. Perform the test with these speeds:

5 km/h	walking speed
36 km/h	by car

B: (z3→z1)
Start inside a negative VA. Walk toward the boundary of a positive VA in a constant speed. Measure the distance to the boarder at the time the user is granted access. Repeat 5 times for each speed and calculate the mean. Perform the test with these speeds:

5 km/h	walking speed
36 km/h	by car

4.1.5 Integrity test

A: (z1→z3→z1)
The test defined in 4.1.2 and 4.1.3 deals with only one scenario at a time. The purpose of this test is to combine these two together. Start inside zone 1. Walk toward the boundary of a negative VA in a constant speed. Cross the boundary and walk into zone 3.Once inside the zone 3, turn around and walk back to zone 1. The test will verify if the demonstrator is capable of controlling the access of a UE moving from valid area into invalid area and return back to start point.

B: (z1→z3→z1)

The test defined in 4.1.2 and 4.1.3 deals with only one scenario at a time. The purpose of this test is to combine these two together. Start inside zone 1. Walk toward the boundary of a negative VA in a constant speed. Cross the boundary and walk into zone 3.Once inside the zone 3, turn around and walk back to zone 1. The test will verify if the demonstrator is capable of controlling the access of a UE moving from invalid area into valid area and return back to start point.

4.2 Test results

4.2.1 Always inside

Figure 36 shows the distance between UE and the boarder of the VA. It also shows the leasing time given and whether UE is authenticated or not. The data behind the graph is found in Parameter_Test_1.xls. During the first period, the UE is standing still. After a while UE starts moving around within zone 1. The UE is given a positive leasing time throughout the entire test period.

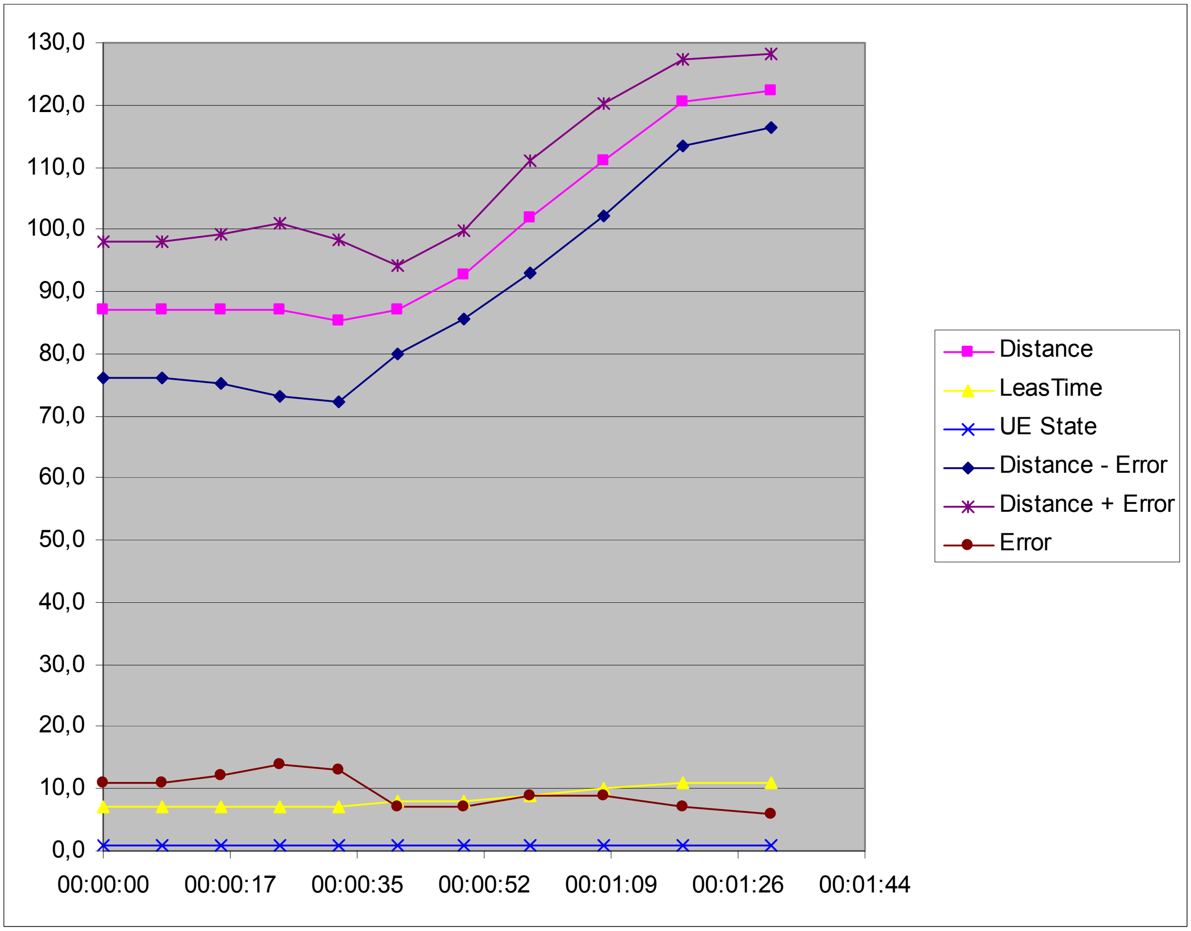


Figure 36 - Always inside

4.2.2 Always outside

Figure 37 shows the distance between UE and the boarder of the VA. It also shows the leasing time given and that the UE is always denied access. The data behind the graph is found in Parameter_Test_2.xls. During the first period, the UE is moving. After a while the UE stops, ands stays still within zone 3. The UE is given a leasing time of zero throughout the entire test period.

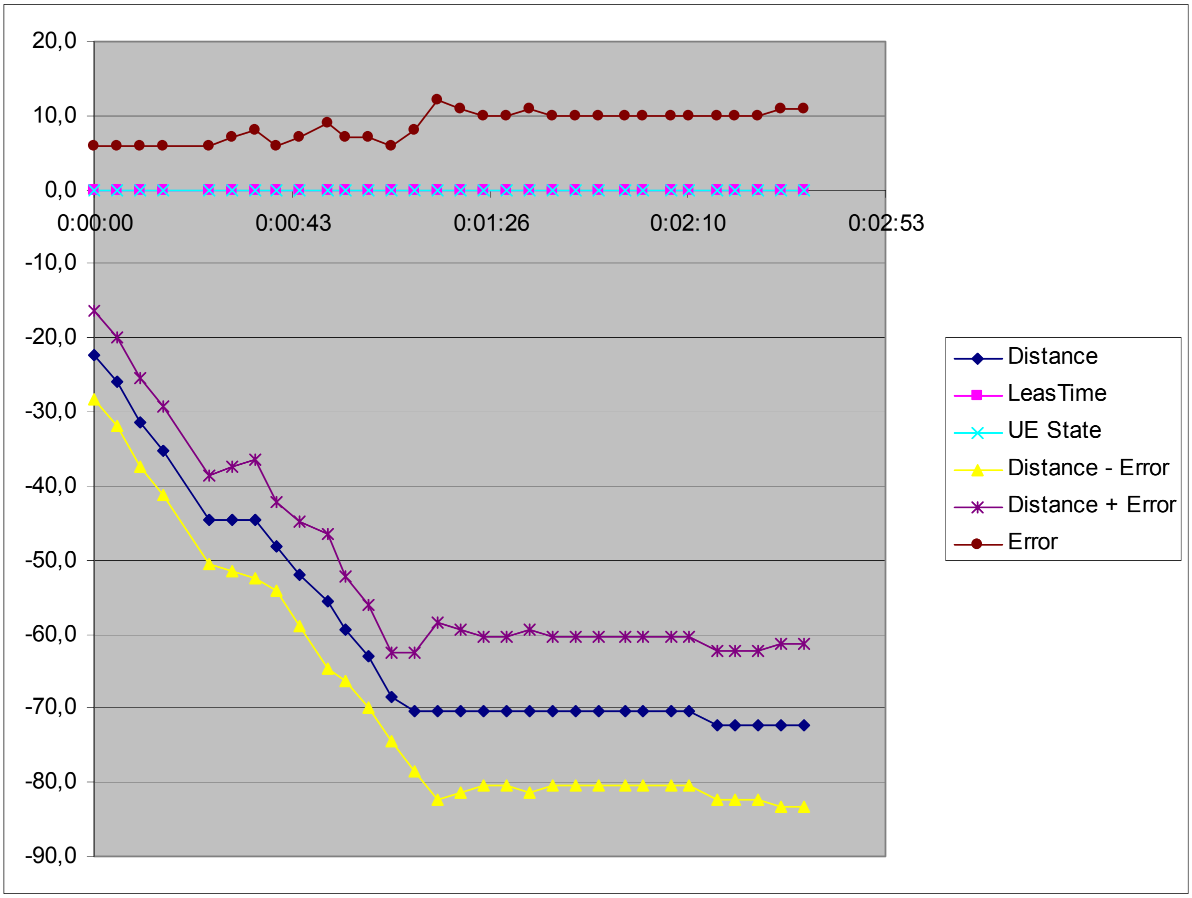


Figure 37 - Always outside

4.2.3 Crossing boundary

A (z1 → z3):

Figure 38 shows that as the UE moves closer and closer to the boarder from zone 1 towards zone 3, the leasing times drops. At a certain distance, the UE enters zone 2, and is denied access. This happens before the UE enters zone 3. The test in Figure 38 is carried out with the UE moving at approximately 5 km/h. The data is found in Parameter_Test 3a_5kmh_2.xls.

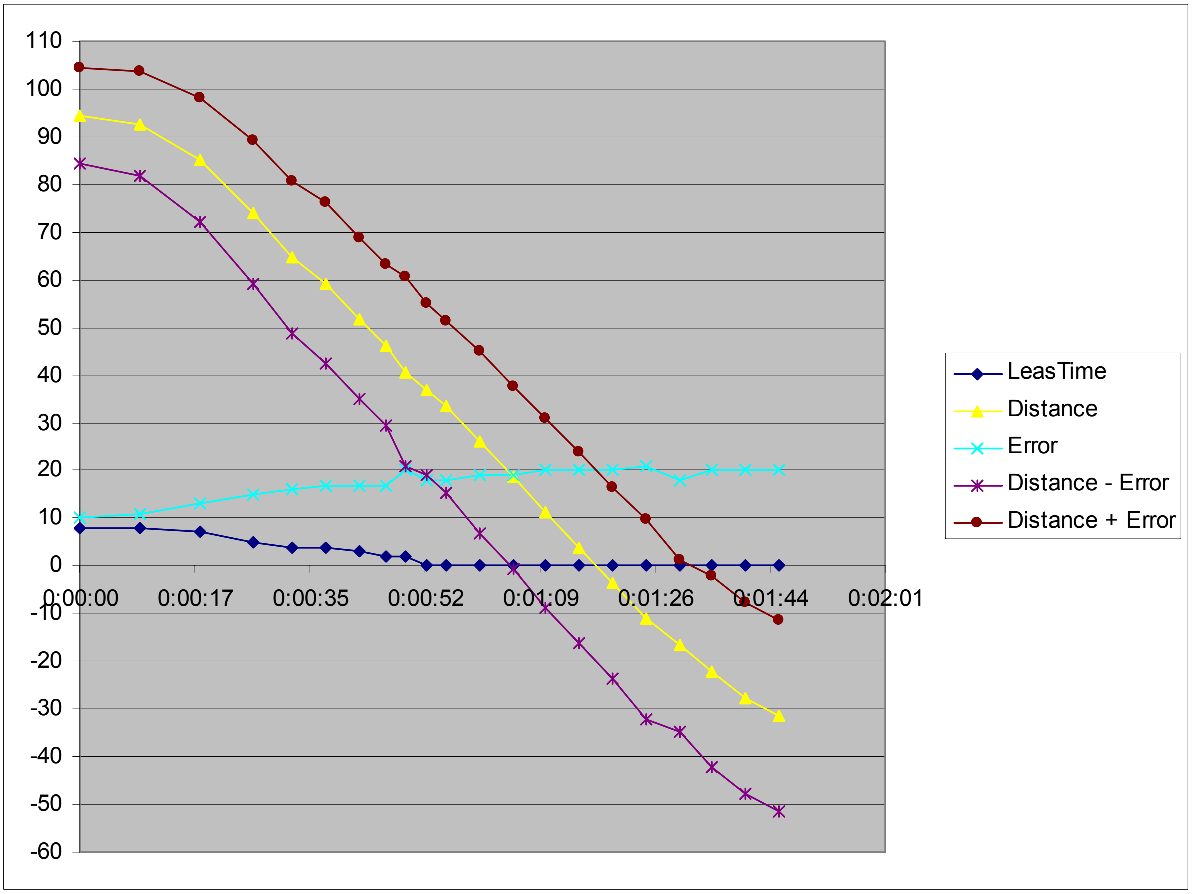


Figure 38 - Crossing boundary z1 → z3

The average distance where UE is denied access, giving a leasing time of zero, is approximately 19 meters. This is calculated by subtracting the error from the distance in the data collection. Then the average is calculated over the three tests. The average velocity around the point of measurement, including the pre- and post-measurement is included.

Table 9 - Average distance z1 → z3 5km/h

Test name	Distance – Error (m)	Velocity (km/h)
Parameter_Test_3a_5kmh_1	20	5
Parameter_Test_3a_5kmh_2	19	5
Parameter_Test_3a_5kmh_3	19	4
Average	19	5

The test was repeated near the speed limit of 36 km/h. UE was denied access at an average distance of about 8 meters.

Table 10 - Average distance z1 → z3 36km/h

Test name	Distance – Error (m)	Velocity (km/h)
Parameter_Test_3a_35kmh_1	10	34
Parameter_Test_3a_35kmh_2	7	34

Parameter_Test_3a_35kmh_3	12	32
Parameter_Test_3a_35kmh_4	7	33
Average	9	33

B (z3 → z1):

Figure 39 shows that as the UE crosses the boarder from zone 3 towards zone 1, the leasing times stays zero until the UE crosses the point of zone 2 described in formula [II]. At this point the UE is granted access. The test in Figure 39 is done with the UE moving at approximately 5 km/h. The data is found in Parameter_Test_3b_5kmh_2.xls.

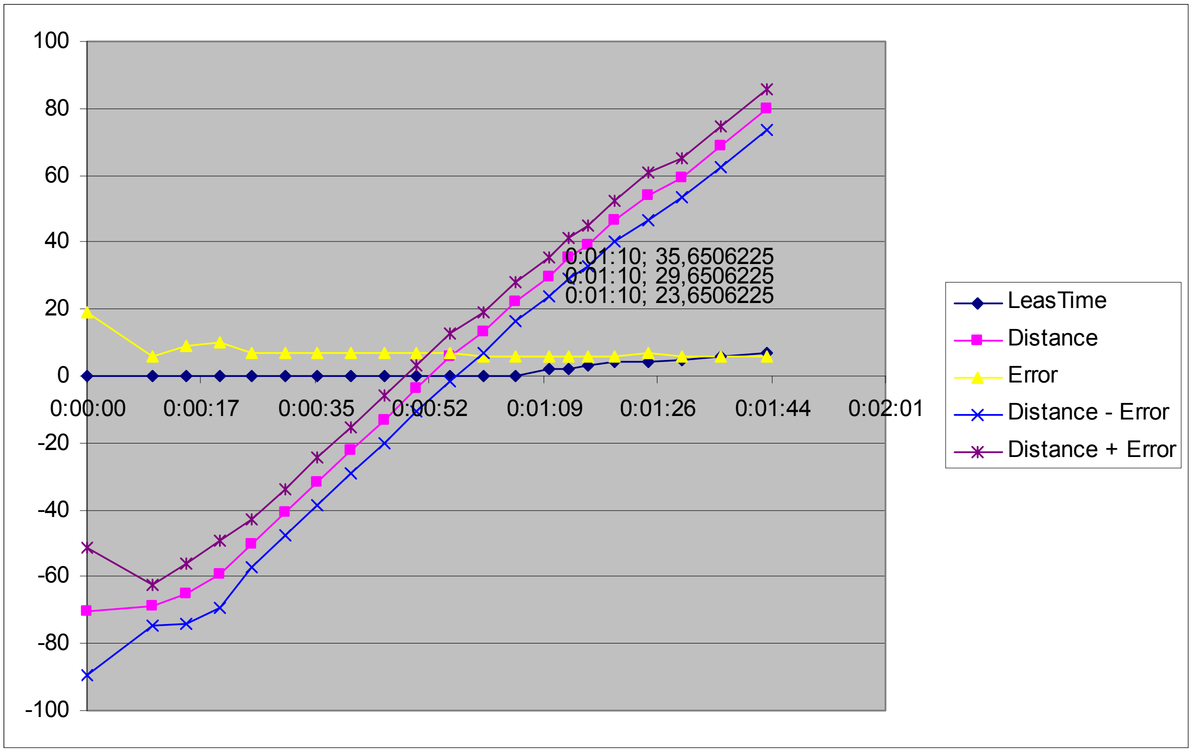


Figure 39 - Crossing boarder z3→z1

The average distance at which the UE is granted access is about 24 meters with a velocity of approximate 5 km/h.

Table 11 - Average distance z3-z1 5 km/h

Test name	Distance – Error (m)	Velocity (km/h)
Parameter_Test 3b_5kmh_1	22	5
Parameter_Test 3b_5kmh_2	24	5
Parameter_Test 3b_5kmh_3	27	6
Average	24	5

When UE is traveling at near max speed, the average distance at which UE is granted access is 38 meters.

Table 12 - Average distance z3 → z1 36 km/h

Test name	Distance - Error (m)	Velocity (km/h)
Parameter_Test 3b_35kmh_1	51	34
Parameter_Test 3b_35kmh_2	41	33
Parameter_Test 3b_35kmh_3	33	35
Parameter_Test 3b_35kmh_4	27	34
Average	38	34

4.2.4 Integrity test

A (z1 → z3 → z1):

In Figure 40 the UE is starting in zone 1 moving towards zone 3. After crossing the boundary, UE continues for a while, turns around, and starts moving towards zone 1 again. The graph shows that the leasing time diminishes as the UE moves closer to the boundary. When measured within zone 2, UE is denied access with a leasing time of zero. The leasing time stays at zero until UE is again measured inside zone 1. The point of entering zone 2 happens at 1:17 roughly at 20 meters. After turning around, walking towards zone 1, UE is granted access at about 23 meters. The data is found in Parameter_Test_4a_1.xls

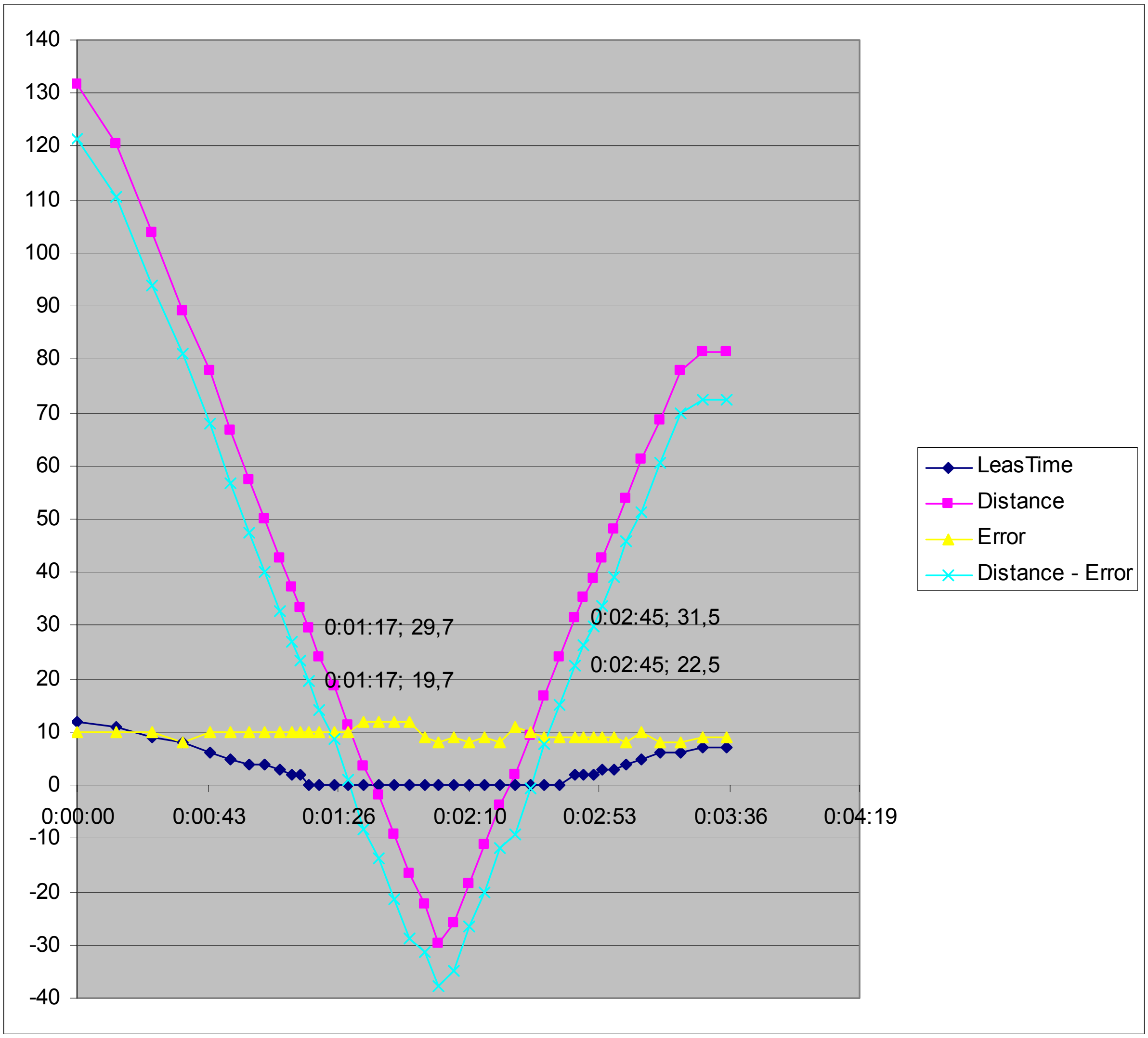


Figure 40 - Integrity test z1 → z3 → z1

B (z3 → z1 → z3):

In Figure 41 the UE is starting in zone 3, with no access, moving towards zone 1. After crossing the boundary, UE continues for a while, turns around, and starts moving towards zone 3 again. The graph shows that UE has a constant leasing time of zero until reaching within zone 1. As UE moves further into zone 1, the leasing time increases. When measured within zone 2, UE is again denied access with a leasing time of zero. The point of gaining access happens at 1:00 at almost 30 meters. After turning around, walking towards zone 3, UE is denied access at 13 meters. The source of these data can be found at Parameter_Test_4b_1.xls.

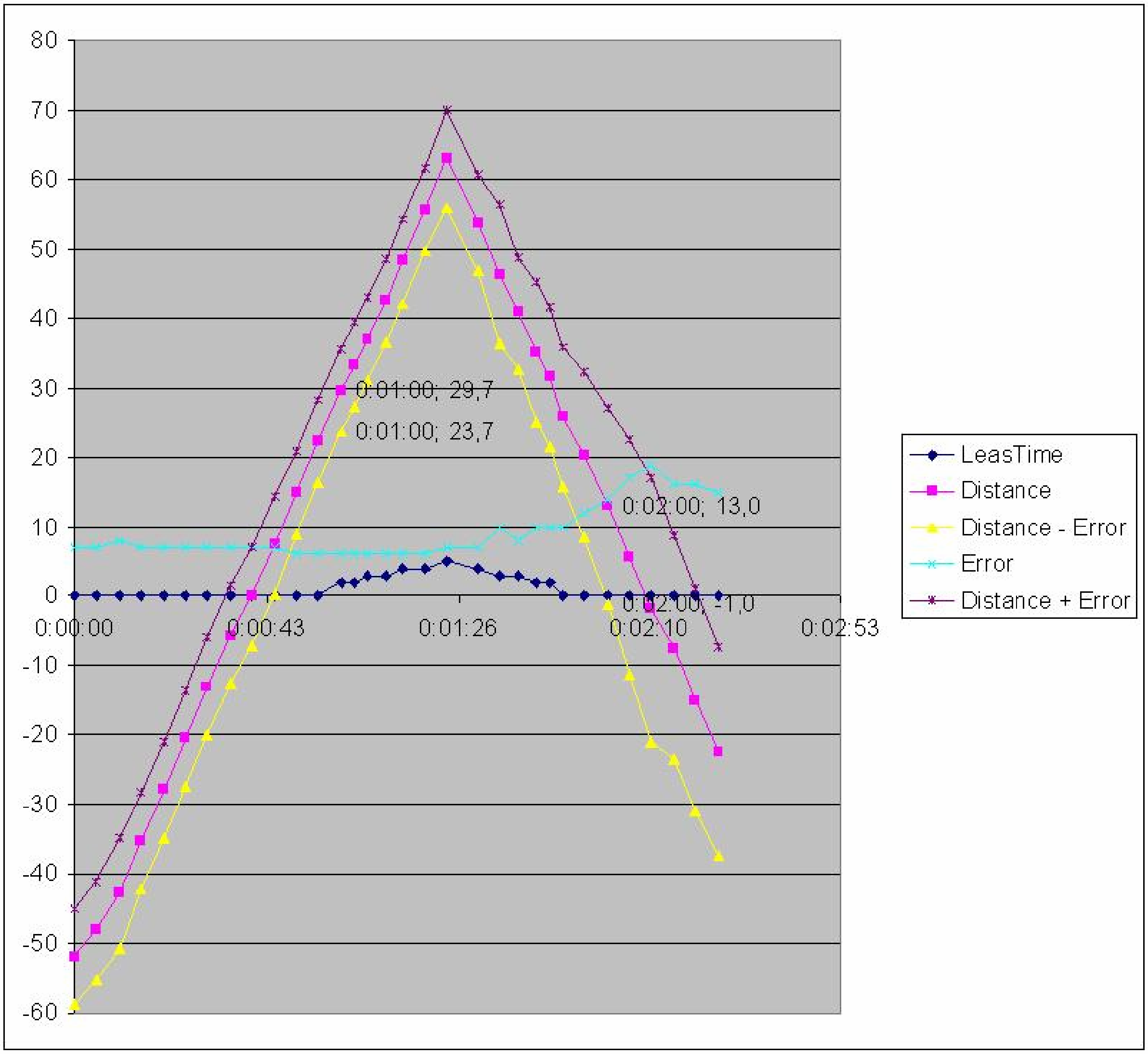


Figure 41 - Integrity test z3 → z1 → z3

5 Discussing the results

5.1 Always inside

In this test the UE is moving entirely inside a valid area. The test results show that the UE is granted access throughout the entire test period. This shows that the system behaves correctly when inside a valid area. The position measurements are done with different intervals dependant on the leasing time given. The leasing time increases as the distance to the boundary increases. The system works both while the UE is standing still and while moving around inside the VA.

5.2 Always outside

This test investigates how the system behaves when the UE is entirely within an invalid area. As the graph shows, the leasing time is zero throughout the entire test period. The UE is denied access within the invalid area. The system works properly both while UE is moving around and standing still.

5.3 Crossing boundary

A (z1→ z3):
If UE is crossing the boundary from zone 1 towards zone 3 it will be denied access. Figure 38 shows that the leasing time is dropping as the UE gets closer to the boundary of zone 1. At one point, approximately at a distance of 19 meters to zone 3, the UE is locked out. This is accordingly to the theory of the size of zone 2 (See chapter 2.7.2.3). There is a probability for the UE to be measured within zone 2 but it will be denied access if made so. Zone 2 starts at 20 meters using formula [II]. This test clearly shows that the system is capable of denying a user access according to its position.

The average distance where the UE is denied access is 19 meters. According to formula [II] UE can be denied access already at 20 meters. The UE is in this case only moving at a speed of 5 km/h. This is less that the maximum speed used for calculations on denying access. The speed used is 36 km/h. This means that if UE is measured just outside the 20 meter boundary for zone 2, it is theoretically possible for UE to move 20 meters towards the boundary of zone 3 within the next position measurement. In this test UE is only moving at 5 km/h. Table 9 shows that UE is already denied access at approximately 19 meters. We can see from the test where UE is moving at a speed closer to the maximum speed, that the theory is correct. Table 10 now shows an average distance of around 8 meters.

B (z3→ z1):
In this test UE starts in an invalid, zone 3, and starts moving closer and closer towards the boundary, eventually crossing it. The first measurement, after crossing the boundary between zone 2 and zone 1, grants UE access with a positive leasing time. UE checks its position every 5 seconds when not authenticated. Every 5 seconds an entire authentication procedure is performed. As we see from the graph, there are many measurements done prior to the UE getting into zone 1. This may be improved by using a leasing time for how often the AKA procedure should be performed when outside zone 1. This can be based on the same formula [IV], but instead of measuring distance to nearest invalid area, measure the distance to the nearest valid area. It is not as crucial to grant access as it is to deny access fast.

Table 11 shows that UE is granted access at an average distance of approximately 24 meters traveling at a speed of 5 km/h. This is close to the theoretical distance of 20 meters. With higher speeds, the average distance gets larger. As Table 12 shows at around 34 km/h the average distance where UE is granted access is 41 meters.

With small Validity Areas where the zone 2 size is large in proportion to zone 3 and zone 1, this may have important consequences. But with Validity Areas in the sizes of kilometers it will not be as significant. On the other hand, using 3G systems with cells of that magnitude also allows for user speeds in the range of what is proposed in 2.7.2.1. This will give a grey-zone of approximately 200 meters.

5.4 Integrity test

A:
Test 1, always inside has already established the fact that whenever UE is given a positive leasing time, UE is granted access. This test shows that the system handles well the transition between zone 1 into zone 3 and back into zone 1. The test shows that UE is granted access as long as it stays in zone 1, and regains access after a period of no access.

B:
This also works when starting within zone 3, moving into zone 1 and back into zone 3. The system correctly denies access in zone 3 and whenever measured within zone 2. UE is granted access whenever in zone 1.

5.5 Adding a spatial dimension

Adding a spatial dimension gives the operators better control of their own system. They can control their subscriber's whereabouts. This raises an issue of privacy. The subscriber may not want to expose to the operator where he/she has been at all times. On the other hand, the lack of privacy can be considered less a drawback than the benefits of adding such a system. The subscribers must be aware of to what extent they are being tracked, how long this data is stored, and who can gain access to the data. Another benefit of adding a spatial dimension is the way the operators can control their roaming partners. This does not have to affect the users at all, but merely give the operators a way to control that the roaming contracts are being held. To achieve spatial control, the operators have to invest a lot of money in a position measuring infrastructure. Given the E911 and E112 requirements from the governments in both US and EU, building an infrastructure is forced to come. This will be implemented in the access networks, including using the user equipment for measuring. The requirements of accuracy do not force an integration of GPS in every mobile terminal. But, as position data is becoming a standard feature, soon there will be many interested parties offering different location based services. Mobile terminals are constantly being equipped with more and more technology. A GPS module in every mobile terminal may not be as far into the future as one would think. Implementation of positioning equipment is expensive, independent of where it is implemented. What might seem as a large investment is in fact a possibility for future income. It is important that the operators see the potential in the investment and not only the costs. They should instead focus on development of software and services that makes use of the new possibilities.

An essential question raised after gaining some experience with the spatial AKA is; Is the AKA procedure the correct place for spatial information to be placed? There are several possible places for this to be implemented, all depending on the different usage of such information. The information can be used in conjunction with the authentication process. This will control the user in the initial phase. If denied access, the resources are freed at an early stage. [Køien, Oleshchuk, 2003] suggests a system where the position data is implemented in the challenge response messages of the AKA. This postulates that the Area Descriptors should be at least the size of the native authentication area. The work of this paper has shown a system where the Area Descriptors are independent of the coverage of the access network, or the size of the authentication area. The costs of such a system are the increased signaling load and the added computation in HE. Given the goal of adding spatial control, it might be more convenient to add the position checking in conjunction with services. This still gives home control, but instead of adding control to the authentication phase, it controls the use of services. This principle allows for a more differentiated control of the subscribers. It is possible to deny one service, and still allow another. The positioning data may also be used in conjunction with Role Based Access. E.g. a person is logged in with the role doctor. Because he is a doctor, he gets access to all the medical records. Adding a spatial dimension to the access control system gives him or her access to medical data because he or she is a doctor, but only if located at the hospital. He will not gain access logging in from the local pub in his spare time. Many new applications will spawn because of the ability to use position data. Position aware applications are already tried out in minor scales.

6 Concluding marks

The main goal of this thesis was to develop an experimental system. The system should implement a spatial exposure control in conjunction with a 3G access authentication system. By adding position checking and validation against a position database, we have proven that such a system is realizable with little changes to the UMTS AKA procedure.

Tests have verified a demonstrator capable of granting and denying access based on the position of the user equipment during the execution of AKA. Tests state that access is denied at a 100 % rate in invalid areas.

A leasing time is calculated if the position is found valid. The leasing time indicates how long the measurement is valid and when UE should perform a new position measurement. This preserves battery while signaling load is kept at a minimum.

A theory of sizes and measures of critical parameters is developed. The tests results verify that the chosen values give good results. The system model has it strengths and weaknesses. High accuracy makes it possible to deny access in small areas, but at a cost of a rather large grey-zone where the user may be situated, but is denied access if ever measured there.

The demonstrator does not implement any privacy preserving techniques, but a system like the S2PLIP is suggested.

The spatial dimension gives HE more control over its subscribers. The operators must see the business potential in the new technology, and not hide behind a tight budget refusing to invest in position equipment. With spatial AKA, HE will also gain more control of the roaming partners, as billing records can be independently validated.

We have seen the potential in adding a spatial dimension to the AKA. Still, this is very limiting. What this feature is providing is mostly access control and monitoring possibilities. By moving the spatial control to e.g. the service level, HE will have a more differentiated control.

References

3GPP TS 22.016, International Mobile Equipment Identities (IMEI).

3GPP TS 23.002, Network architecture.

3GPP TS 23.060, General Packet Radio Service (GPRS); Service description; Stage 2.

3GPP TS 24.008, Mobile radio interface Layer 3 specification; Core network protocols; Stage 3.

3GPP TS 25.305, User Equipment (UE) positioning in Universal Terrestrial Radio Access Network (UTRAN); Stage 2.

3GPP TS 25.882, 1,28 Mcps TDD option base station classification.

3GPP TS 29.002, Mobile Application Part (MAP) specification.

3GPP TS 33.102, 3G security; Security architecture.

3GPP TS 33.234, Wireless Local Area Interworking Security.

3GPP TS 35.201, Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications.

3GPP TS 35.202, Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification.

3GPP TS 35.203, Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data.

3GPP TS 35.204, Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data.

3GPP TS 35.206, 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification.

3GPP TS 35.207, 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data.

3GPP TS 35.208, 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data.

Ackerman, M. S., Privacy in E-commerce: Examining user scenarios and privacy preferences, In Proceedings of Elecronic Commerce, 1999.

Barkuus, L. and Dey, A., Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns, Intel Research Berkeley, 2003.

CGALIES, [ONLINE], http://www.telematica.de/cgalies/, accessed on February 2004.

Hatfield, D. N., A Report on Technical and Operational Issues Impacting The Provision of Wireless Enhanced 911 Services, Federal Communications Commission, 2002.

Kaplan, E. D., *Understanding GPS, Principles and Applications*, Artech House Publishers, Boston, 1996.

Køien, G. M., *An introduction to access security in UMTS*, IEEE Wireless Communications magazine, February 2004.

Køien, G. M. and Oleshchuk, V., *Spatio-Temporal Exposure Control; An Investigation of spatial home control and location privacy issues*, In Proceedings of the 14th Annual IEEE Symposium on Personal Indoor Mobile Radio Communications (PIMRC), pp.2760-2764, September 2003.

Llusca, E.; Val, T.; Normand, C.; Mercier, J.J., *Location of mobiles stations in a wireless LAN*, Local Computer Networks, 2000 Proceedings 25th Annual IEEE Conference on , 8-10 Nov. 2000 Pages:165 – 166.

Math World, [ONLINE], http://mathworld.wolfram.com/GreatCircle.html, accessed on February 2004.

MSDN, [ONLINE], http://msdn.microsoft.com/library/, accessed on May 2004.

Porcino, D., Location of third generation mobile devices: a comparison between terrestrial and satellite positioning systems, IEEE Vehicular Technology Conference 53rd, Vol. 4, Pages:2970 – 2974, 6-9 May 2001.

Prasithsangaree P., Krishnamurthy P., Chrysanthis P.K., *On indoor position location with wireless LANs*, The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Pages:720 - 724 vol.2, 15-18 Sept. 2002.

RFC768, User Datagram Protocol, IETF, 1980.

Zhao, Yilin, Motorola Inc., *Standardization of Mobil Phone Positioning for 3G Systems*, IEEE Communications Magazine pp.108-115, July 2002.

The White House, Office of the Press Secretary, Statement by the president regarding the united states' decision to stop degrading global positioning system accuracy, USA, 2001.
[ONLINE] http://www.ngs.noaa.gov/FGCS/info/sans_SA/, February 2004.

Appendix

[A] Parameter test results
Parameter_Test_1.xls
Parameter_Test_2.xls
Parameter_Test_3a_5kmh_1.xls
Parameter_Test_3a_5kmh_2.xls
Parameter_Test_3a_5kmh_3.xls
Parameter_Test_3a_35_1.xls
Parameter_Test_3a_35_2.xls
Parameter_Test_3a_35_3.xls
Parameter_Test_3a_35_4.xls
Parameter_Test_3b_5kmh_1.xls
Parameter_Test_3b_5kmh_2.xls
Parameter_Test_3b_5kmh_3.xls
Parameter_Test_3b_35_1.xls
Parameter_Test_3b_35_2.xls
Parameter_Test_3b_35_3.xls
Parameter_Test_3b_35_4.xls
Parameter_Test_3b_35_5.xls
Parameter_Test_3b_35_6.xls
Parameter_Test_4a_1.xls
Parameter_Test_4a_2.xls
Parameter_Test_4a_3.xls
Parameter_Test_4b_1.xls
Parameter_Test_4b_2.xls
Parameter_Test_4b_3.xls

[B] CD-ROM
Report
Code
Auditory

Appendix A

Appendix B