Project Number	**:**	**AC095**
Project Title	**:**	**ASPeCT : Advanced Security for Personal Communications Technologies**
Deliverable Type	**:**	**P (Public)**

CEC Deliverable Number	**:**	**AC095/ATEA/W21/DS/P/05/A.1**
Contractual Date of Delivery to the CEC	**:**	**Y02 / M06 (August 1996)**
Actual Date of Delivery to the CEC	**:**	**Y02 / M06 (August 1996)**
Title of Deliverable	**:**	**Migration scenarios**
Work packages contributing to the Deliverable	**:**	**WP2.1**
Nature of the Deliverable	**:**	**R (Report)**
Author (s)	**:**	**Geneviève Vanneste, Johan Degraeve (Editors)**

Abstract :

This report outlines possibilities for the migration path from second-generation systems to UMTS, with particular regardto security features.

Some of the factors and parameters affecting the migration path towards UMTS are identified, and a framework to describe the migration towards UMTS security is proposed.

A possible network-based evolution/migration path towards UMTS is described, starting from GSM phase 2 +.

A framework for authentication is described, enabling the on-line setting up of roaming agreements and providing a flexible mechanism to support the multiple authentication mechanisms to be used in UMTS and facilitating migration.

A functional description is given of the starting point, GSM phase 2+, and the target system UMTS, which will support the framework for authentication.

Security features provided in second generation systems are compared to the planned features for UMTS. A proposal to introduce security enhancements in the intermediate levels of the migration path is made.

A functional description of the demonstrator, scheduled for the end of May 1997, is included, together with ASN.1 specifications of most of the exchanged messages.

Key words:
ACTS, ASPeCT, UMTS, Migration, Evolution, Security, Authentication Framework, Roaming agreement

0. Executive Summary

The need for enhanced security features in UMTS has led to the definition of specific security objectives. These objectives have been translated into security requirements, resulting in a classification of security features. Mechanisms to realise the UMTS security features are currently under development. Secret key-based mechanisms, as well as public key-based mechanisms have been proposed for UMTS, providing mutual authentication, cipher key agreement for confidentiality, anonymity and non-repudiation.

To allow a cost-effective introduction of UMTS, migration/evolution scenarios have been defined within ETSI, aiming at a smooth introduction of the new services and systems, starting from existing contemporary mobile and fixed telecommunication systems. However, it is envisaged that the network-based migration process will be affected by a number of factors e.g., "triggering events" (like the introduction of B-ISDN, the UMTS air-interface, etc.), techno-economics, market demands, regulatory issues, etc. It is clear that these factors will not influence all operators in the same way and, as a result, a single migration path cannot be defined.

This deliverable aims to outline possibilities for the migration path from second-generation systems to UMTS, regarding security features. It must stressed though, that security related migration issues cannot be addressed in isolation, but they should be investigated in the context of the overall network-based migration.

Some of the factors and parameters affecting the migration path towards UMTS are identified, and a 'general framework' for the migration of security offered by second generation systems towards UMTS security is proposed.

A possible network-based evolution/migration path towards UMTS is described, starting from GSM phase 2 +. The fundamental assumption is that the evolution/migration path towards UMTS is based on gradual enhancements and exploitation of the GSM infrastructure, thus maximising the use of existing network investments. The described path is based on the ETSI report on 'Scenarios and considerations for the introduction of the Universal Mobile Telecommunications System' [1].

The concept of a framework for authentication is introduced, and its advantages in support of migration towards UMTS are explained. The key points are the concept of user capability classes, user-network (mutual) authentication using negotiated mechanisms and the automatic establishment of Network Operator-Service Provider roaming agreement where required.

A functional description is given of the starting point, GSM phase 2+. The phase 2+ work items defining impact on security are summarised, enhanced with 'candidate' work items, discussed in ETSI SMG10. The target system, UMTS, supporting the framework for authentication, is described by the different operational scenarios. Two main categories for operational scenarios are defined, those that involve a request for user-network authentication, and those that involve a request to establish an Network operator - service provider roaming agreement.

Security features provided in 2nd generation systems are compared to the expected features for UMTS. Two approaches for introducing these features can be foreseen, evolution (improvement or upgrade) of the contemporary GSM/DECT security features by implementing new, advanced security mechanisms, the second approach is supporting a subset of the security features expected to be offered by the UMTS. A proposal to introduce security enhancements in the different intermediate levels of the migration path is made.

A functional description of the demonstrator, scheduled for the end of May 1997, is included. This demonstrator aims to show the validity of the UMTS migration protocol and the feasibility of implementing a migratory UIM. In the first demonstrator a simplified version of the migration scenarios will be implemented. The feasibility of adding the authentication framework, together with UMTS authentication protocols will be showed. The ASN.1 specifications of most of the exchanged messages are provided in the last part of this deliverable.

List of Contents

List of figures

List of Tables

1. Introduction

This report aims to outline possibilities for the migration path from second-generation systems to UMTS, regarding security features.

In chapter 3 some of the factors and parameters, affecting the migration path towards UMTS are identified, additionally a framework used to describe the migration towards UMTS security is proposed.

A possible network based evolution/migration path towards UMTS is described in chapter 4, starting from GSM phase 2 +.

A framework for authentication is defined in chapter 5, enabling the on-line agreement of roaming agreements and providing a flexible mechanism to support multiple authentication mechanisms to be used in UMTS and facilitating migration.

A functional description is given of the starting point, GSM phase 2+ (chapter 6), and the target system, supporting the framework for authentication, UMTS (chapter 7).

Security features provided in 2nd generation systems are compared to the expected features for UMTS. A proposal to introduce security enhancements in the different intermediate levels of the migration path is made.(chapter 8)

A functional description of the demonstrator, scheduled for the end of May 1997, is included (chapter 9), together with ASN.1 specifications of most of the exchanged messages (chapter 10).

1.1 Contributors

This deliverable has been composed by following partners: Siemens Atea, Panafon and Vodafone.

Hereafter follows the list of all project managers involved in the ASPeCT project plus the principal editors (Johan Degraeve and Geneviève Vanneste) whose contact details are included.

Bart Preneel	ESAT/COSIC KU Leuven K. Mercierlaan 94 B 3001 Heverlee Belgium	Phone: +32 16 32 1148 Fax: +32 16 32 1986	bart.preneel@esat.kuleuven.ac.be
Yannis Vithynos	PANAFON 2 Mesogeon Avenue 11527 Athens Greece	Phone: +30 1 64 07 267 Fax: +30 1 64 07 039	vithynos@panafon.gr
John Shawe-Taylor	Royal Holloway, University of London Egham Surrey TW20 0EX England	Phone: +44 1784 44 34 30 Fax: +44 1784 43 97 86	jst@dcs.rhbnc.ac.uk
Guenther Horn	Siemens AG ZFE T SN 3 D-81730 München Germany	Phone: +49 89 636 41494 Fax: +49 89 636 48000	Gunther.Horn@zfe.siemens.de
Geneviève Vanneste	Siemens Atea Atealaan 34 B-2200 Herentals	Phone: +32 14 252937 Fax: +32 14 253339	p82586@vnet.atea.be

	Belgium		
Johan Degraeve	Siemens Atea Atealaan 34 B-2200 Herentals Belgium	Phone: +32 14 252431 Fax: +32 14 253339	p82953@vnet.atea.be
Eric Johnson	GIESECKE & DEVRIENT GMBH Prinzregenstr. 159 D-81607 München Germany	Phone: +49 89 4119 944 Fax: +49 89 4119 905	X400: c=de; a=cwmail; p=g+d; s=johnson; g=eric Internet: 100277.1206@compuserve.com
Nigel Jefferies	Vodafone Ltd The Courtyard 2-4 London Road Newbury Berks RG14 1JX England	Phone: +44 1635 503883 Fax: +44 1635 31127	Nigel.Jefferies@vf.vodafone.co.uk
Martin Urch	HAINES WATTS CONSULTING Sterling House 1 Loughborough Road West Bridgford Nottingham NG2 7LJ England	Phone : +44 115 945 5333 Fax : +44 115 982 1430	100307.3052@compuserve.com
Roddi Coudron	LERNOUT & HAUSPIE Sint-Krispijnstraat 7 B-8900 Ieper Belgium	Phone : +32 57 22 88 89 Fax : +32 57 20 84 89	roddi.coudron@lhs.be

1.2 Document History

Revision	Date	Changes
A	14/03/96	First Draft containing some preliminary thoughts on migration scenarios
B	30/04/96	Draft for review by ASPeCT
C		First Draft containing full table of contents after discussion during Forum Meeting in Athens and a few scopes for the chapters. Eventual revision remarks are modifications made by the editor to the input from the contributors.
D	20/06/96	Second Draft containing full table of contents and scopes for the sections.
E	09/07/96	Internal update of the draft
F	19/07/96	First Draft for D05, distributed for review in WP21
G	09/08/96	Internal update
H	20/08/96	Second Draft for D05
I	26/08/96	Third Draft for D05, distributed to all ASPeCT partners
1	30/08/96	Final Version

2. Abbreviations

AC	Authentication Centre
ASN.1	Abstract Syntax Notation Number 1
B-ISDN	Broadband-Integrated Services Digital Networks
BSC	Base Station Controller
BSS	Base Station System
BSSMAP	Base Station System Mobile Application Part
BTS	Base Station Transceiver
CA	Certification Authority
CAMEL	Customised Applications for Mobile network Enhanced Logic
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CEC	Commission of the European Communities
CI	Cordless Interface
CKSN	Cipher Key Sequence Number
CS-x	Capability Set-x
CSS	Cell Site Switch
DCS	Digital Cellular System
DCS180	Digital Cellular System at 1800 MHz
DECT	Digtal Enhanced Cordless Telecommunications
DECT FP	DECT Fixed Part
DECT PP	DECT Portable Part
DES	Data Encryption Standard
DSS	Digital Signature Standard
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FAC	Final Assembly Code
FP	Fixed Part
FSM	Finite State Machine
GPRS	General Packet Radio Services
GSM	Global System for Mobile communications
GSM900	Global System for Mobile communications at 900 Mhz
GUI	Graphical User Interface
HLR	Home Location Register
HPLMN	Home PLMN
IC	Intelligent Card
ICR	Intelligent Card Reader
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IMTI	International Mobile Terminal Identity
IMUI	International Mobile User Identity
IN	Intelligent Network
IP	Internet Protocol
IWU	InterWorking Unit
Kc	Ciphering Key
Ki	Subscriber Authentication Key
KUL	Katholieke Universiteit Leuven
LAC	Location Area Code
LAI	Location Area Identification
LE	Local Exchange
MAP	Mobile Application Part
MCC	Mobile Country Code
MNC	Mobile Network Code
MoU	Memorandum of Understanding
MS	Mobile Station
MSC	Mobile Services switchingCentre
MSIN	Mobile Subscriber Identification Number
MT	Mobile Terminal
NO	Network Operator
NOID	Network Operator Identification

OS	Operating System
PBX	Private Branch eXchange
PC	Personal Computer
PDU	Protocol Data Unit
Ph2	Phase 2
PK	Public Key
PLMN	Public Land Mobile Network
PP	Portable Part
RAND	Random Number
RHUL	Royal Holloway University of London
RIL3	Radio Interface Layer 3
RND_N	Random Number generated by the network operator
RR	Radio Resource
RSA	Rivest, Shamir and Adleman
SCP	Service Control Point
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMG	Special Mobile Group
SMS	Short Message Service
SNR	Serial Number
SP	Service Provider
SPID	Service Provider Identification
SRES	Signed Response
TAC	Type Approval Code
TCP	Transmission Control Part
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
TMUI	Temporary Mobile User Identity
TMUIn	Temporary Mobile User Identity generated by the network operator
TMUIs	Temporary Mobile User Identity generated by the service provider
TTP	Trusted Third Party
TUID	Temporary User Identity
UIM	User Identity Module
UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunications
UUS	User to User Signalling
VLR	Visitor Location Register

3. Security Migration Related Aspects

The scope of this section is two-fold: (a) to identify some the factors and parameters that could affect the GSM network-based migration path towards UMTS and (b) to provide a framework for the migration of security offered by contemporary second generation networks towards UMTS security.

3.1 On the Derivation of Migration Scenarios

In this section, a generic method regarding the identification of the GSM network-based migration path towards UMTS is described. The fundamental assumption is that the evolution/migration path towards UMTS is based on the gradual enhancement and exploitation of the GSM network components. However, apart from the evolution of the network components (see paragraph 3.1.1.1), the migration process should be seen in conjunction with other factors e.g., triggering events, techno-economics related aspects, market demands, regulatory issues, etc. It is clear that these factors will not influence in the same way all operators, and as result of that, a single migration path cannot be defined.

3.1.1 Involved Entities

The entities involved in the migration process are (see Figure 1):

- the *SIM/UIM*,
- the *mobile terminal equipment*,
- the *access network*[1] and
- the *core network* comprising the backbone network[2] and the service network[3].

From the network operator and service provider viewpoints, and as far as the investments required for the infrastructure upgrade are concerned, the main entities are: (a) the access network, (b) the backbone network and (c) the service network.

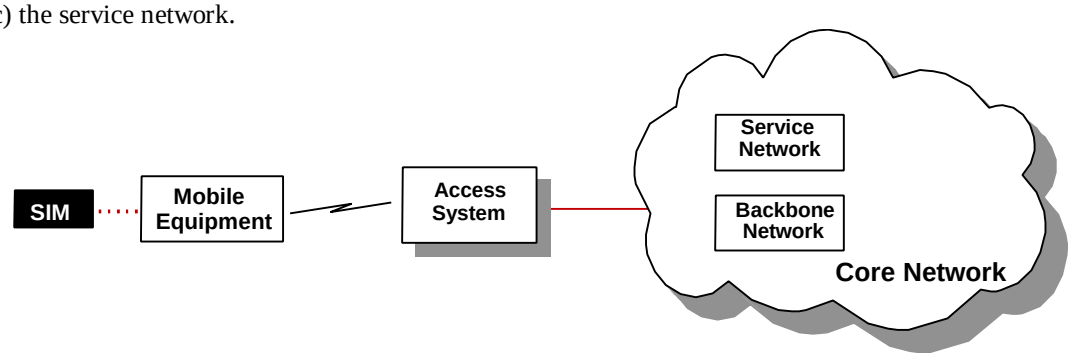


Figure 3-1: The Entities Involved in the Migration Process

3.1.1.1 Evolution Path of the Involved Entities

Table 1 depicts the possible evolution of the entities depicted in Figure 1 in terms of “evolution levels”. The characteristics of the various evolution levels are described below.

A. SIM

The SIM evolution considers the development of GSM/DCS SIM to meet the requirements of the new DECT and UMTS users. Prior to the existence of multi-application SIMs (UMTS/GSM/DCS/DECT), single-application SIMs will be available. However, from the user viewpoint, it would be desirable to be able to use the same SIM to access various terminal types - and thus different networks (with different services and features, quality of service, charging policies, etc.). For instance, the use of a GSM SIM in a DECT terminal will offer

---

1 The access system provides the radio functions i.e., basic transmission and local switching functionality enabling access of mobile terminals to the fixed network resources via the radio interface.

2 The backbone network provides the basic fixed network switching infrastructure and network resources i.e., call and connection control.

3 The service network which provides for data storage, data handling and processing of service requests from mobile users.

the GSM subscriber the possibility to access both public and private environments -utilising different terminals[4]. This necessitates the production of single-mode terminals which allows the acceptance and identification of various SIM types (single- and multi-application ones). Multi-application (and/or single-) SIMs might be also used in fixed terminals to allow for personal mobility (UPT).

B. TERMINAL

Various single- and multi-mode terminals can be envisaged:

- GSM
- DCS
- GSM/DCS
- DECT
- DECT with DECT/GSM/DCS interworking capabilities
- UMTS
- Adaptive multi-mode terminals combining UMTS, GSM, DCS and DECT technologies

In general, each of the above terminal types may accept more than one SIM type e.g., a DECT terminal may also accept GSM SIMs. Multi-mode terminals will possibly accept all the available SIM types.

C. ACCESS SYSTEM

Prior to the introduction of the UMTS BSSs various access systems can be met, for example:

- GSM BTSs and GSM BSCs.
- DCS BTSs and GSM Ph2(+) BSCs (supporting also DCS functionality).
- DECT FPs interconnected to IWUs (required for the interworking with the GSM core network).
- DECT FPs+ with DECT/GSM interworking functionality, interconnected to the GSM core network via concentrators.
- Combinations of the above mentioned access systems.

D. CORE NETWORK

The GSM core network functionality will be gradually upgraded so as to meet the UMTS requirements. The enhancements involve both the GSM MSC/VLR and the GSM HLR/AC/EIR.
The existing MSC/VLRs will be evolved to Ph2(+) MSC/VLRs, so as to support additional access systems attached to it (DCS, DECT and possibly UMTS) as well as to support interworking with the (GSM) IN-SCP. The interface between the Ph2(+) MSC/VLR and the GSM-SCP will be gradually altered from IN/CS-1 to IN/CS-3 subset together with the advancing CAMEL. The evolutionary Ph2(+) MSC/VLR is also likely to support ATM resources and ultimately ATM switching. B-ISDN LE+(s)[5] will be introduced for the interconnection of UMTS BSSs in a matured UMTS system.

E. SERVICES and FEATURES

The set of services and features offered nowadays by the existing GSM systems will be further developed by the introduction of DCS and DECT (high bit rate data services in both public and private environments), to a much wider set of novel services and features (UMTS services) including multimedia, videotelephony, broadband data services, etc.

SIM TYPE	TERMINAL TYPE	ACCESS SYSTEM	SWITCHING NETWORK	SERVICE NETWORK
GSM	GSM MS	BTS(GSM) ⊕ BSC(GSM)	MSC/VLR	HLR (GSM)
DCS	DCS MS	BTS (DCS) ⊕ Ph2 BSC(GSM)	Ph2 MSC/VLR	SCP (GSM)
DECT	DECT PP	BTS (DCS) ⊕ Ph2+ BSC(GSM)	Ph2+ MSC/VLR	SCP (GSM-UMTS)

4 For DECT terminals, care has been taken so as to allow the use of GSM (and probably DCS) SIMs.

5 The notation "+" implies support of UMTS mobility.

GSM/DCS/DECT	GSM/DCS/DECT	FP (DECT) ⊕ IWU	LE+ (B-ISDN)	SCP (UMTS)
UMTS/GSM/ DCS/DECT	UMTS/GSM/ DCS/DECT	FP+(DECT) ⊕ Concentrator		
		BTS (UMTS) ⊕ BSS (UMTS)		
where, the symbol "/" means "and/or" while the "⊕" means "connected to".				

Table 3-1: Possible Evolution of Entities Involved in the Migration Process (non-exhaustive list).

Note 1: The entities' list is a non-exhaustive one.

Note 2: The interconnection of various elements ("evolution levels") -horizontal view- may require the use of IWUs. The note refers to "main entities" only.

3.1.2 Identification of Migration Scenarios

3.1.2.1 Based on Triggering Events

Migration scenarios can be defined based on certain "transition stages" [1]. A transition stage may be based on a pivotal triggering event, occurred either in the access system or in the core network[6]. Among the triggering events, the following could be included:

- the integration of GSM HLR/VLR (towards the IN-SCP)
- the introduction of the DECT radio interface (DECT CI (Cordless Interface))
- the use of B-ISDN in the core network
- the introduction of the UMTS radio interface, etc.

A rational sequence of such triggering events would indicate a specific migration path towards UMTS. Based on the required "main entities" functionality/capabilities, the relevant network components could then be selected from Table 1.

3.1.2.2 Based on Associations between Entities

Migration scenarios could be identified based on rational ***horizontal*** associations between the "evolution levels" of the various entities shown in Table 1. It is obvious that not all combinations are possible. **For example**, the selection of a GSM MSC/VLR precludes the use of UMTS access system. Based on the above observation, a reasonable way to be followed for the identification of the possible migration phases is the selection of the core network functionality (service and switching network capabilities), prior to the selection of the access system. Finally, the corresponding terminal and SIM types can be selected mainly based on the available access systems.

3.1.2.3 Based on Techno-Economics Related Aspects

Migration scenarios could be defined based on considerations regarding the availability of a certain entity "evolution level" in conjunction with the investments (and the expected profit) required for the network upgrade. For example, the introduction of IN-functionality (IN-SCP) might need less investments than the installation of several DECT FPs and the corresponding IWUs.

3.1.2.4 Based on Market Drive

Consumer recognisable and easy-to-use services and end-user products will enable the emergence of a mass consumer market for UMTS [2]. The emergence and specific needs (e.g., broadband multimedia services,

6 However, such a triggering event will -possibly- stimulate the evolution of SIMs and/or terminals. In general, the elaboration of a single entity cannot be examined independently of the others.

satellite services, single terminal equipment for various environments, etc.) could dictate a specific migration path to be followed.

3.1.2.5 Based on Regulatory Issues

Regulatory aspects (frequency allocation, licensing procedures, type approval) can have a significant influence on the migration/evolution process [3]. Issues such as trans-European services and networks, liberalisation and competition in the market, licensing, spectrum and co-operation in research and standardisation to create a unified set of standards could be taken into account during the migration process [2].

3.1.2.6 Combinations of the Above Considerations

Migration scenarios can be also determined taking into account all the above considerations (triggering events, “associations”, availability, investments, legal agreements).

3.2 The Framework for the Migration of Security

The aim of this section is to provide a generic framework for the migration of security offered by second generation networks (GSM, DCS, DECT) towards UMTS security. The framework comprises two general steps:

Step 1. The identification of network-based migration scenarios. The migration scenarios will be based on the evolution of the access and core network, taking into account ETSI's SMG5 work [1]. The output of this step will be a number of "transition phases" separating successive "network levels" as shown in Figure 1.

Step 2. At each "transition phase", the (additional) security features that could be provided by the next network level are investigated. This step includes:

- the identification of the security features that could be provided, taking into account the network capabilities,
- the selection of the mechanisms to support them *(performance and feasibility evaluation)*,
- the definition of security protocols and interfaces,
- the identification of messages exchanged between the various entities (structure and information conveyed),
- the impact on the terminals, SIMs, access and core network functionality, etc.

The outcome of the proposed framework is the identification and definition of the security features and relevant protocols for each "network level" appears in the migration process as described by the migration scenario.

3.2.1 The Framework

A more detailed description of the proposed generic framework is presented in this paragraph. The steps that should be followed are:

STEP 1: Identification and Description of Network-based Evolution/Migration Scenarios

At this step, security related aspects are not the main concern. The definition of the migration scenarios concentrates on network aspects and in particular on the gradual evolution of: (a) the network components and (b) the SIM and terminal types, so as to meet the UMTS functionality and services. ETSI's SMG5 work [1], will be taken into account. However, simplified scenarios will be adopted here. E.g., satellite components could be dropped since satellite related aspects are outside the scope of ASPeCT.

To fulfil this step, the following should be taken into account:

- Definition and Description of the "Initial Network Level" and the "Target Network Level".
- Description of the intermediate evolutionary "network levels".

The description of the network-based evolution/migration scenarios will concentrate on:

- the access system(s) supported,
- the core network capabilities
- the envisaged SIM types
- the envisaged terminal types
- the (user) roaming aspects
- the envisaged services and features, etc.

STEP 2: (Functional) Description of the "Initial Network Level"

This step concentrates on the following issues:

- The identification of the security features that could be supported.
- The identification of the mechanisms to support the selected security features.
- Identification of the interfaces and protocols relevant to security.
- The derivation of the information flows i.e., the definition of the exchanged messages, the message structure and information elements conveyed.

STEP 3: (Functional) Description of the Intermediate "Evolutionary Levels"

At each "transition phase", the following actions take place:

- Investigation of any additional security features that could be supported by the next "evolutionary level".
- Selection of the "appropriate" security mechanisms. The selection will be based on: (a) the available ("proposed") mechanisms and *(b) some evaluation study (performance, feasibility, etc.).*
- Identification of new interfaces and protocols relevant to security.
  (in conjunction with the previous "level" status)
- Derivation of the information flows which comprises, the identification of exchanged messages[7], the message structure and the information elements conveyed.
- Identification of new requirements (security algorithms, functionality, interfaces, protocols) concerning terminals, SIMs, access and core network.

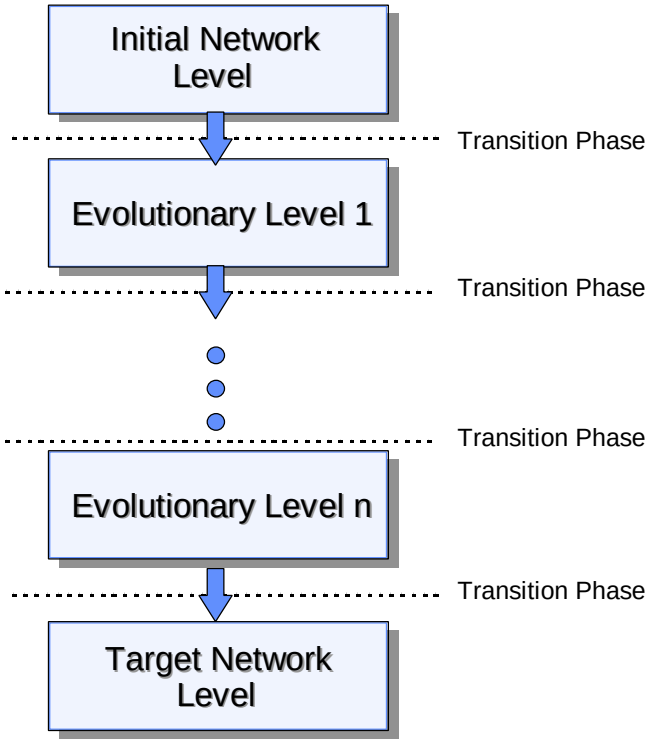


Figure 3-2: "Network Levels" and "Transition Phases"

[7] If previous "level" protocols cannot support new messages, new protocols should be defined.

4. Network-Based Evolution/Migration scenarios

In this section, a possible GSM network based evolution/migration path towards UMTS is described. The fundamental assumption is that the evolution/migration path towards UMTS is based on the gradual enhancement and exploitation of the GSM infrastructure, maximising thus the profits from the network investments. The evolution/migration process involves several entities: the SIM, the mobile terminal, the access network and the core network (comprising the backbone network and the service network), as shown in Figure 4-1.

The described path is based on the described evolution/migration path described in ETR 0104 “Scenarios and considerations for the introduction of the Universal Mobile Telecommunications System (UMTS) [1]”. Two differences between the ASPeCT approach and the ETR 0104 can be observed:

1. The ASPeCT level 1 corresponds to the level 2 of the ETR 0104.
2. The ASPeCT level 2 corresponds to the level 3 of the ETR 0104 but without the introduction of the UMTS air-interface.

The ASPeCT levels 3 and 4 are equal to the corresponding ones of the ETR 0104.

As "initial network level" (ASPeCT level 1), an evolved GSM operator at 900 MHz, supporting also DCS at 1800 MHz and DECT access systems has been considered. ASPeCT level 1 corresponds with level 2 in ETR 0104.

During the evolution/migration path towards UMTS, three evolutionary steps are envisaged:

- In the first evolutionary step (ASPeCT level 1 to ASPeCT level 2) the smart card (SIM) and the home service provider (SCP) are upgraded towards UMTS. A user with a equipped with a new multi-application UIM can use his/her UIM in a real UMTS network as well as in existing GSM/DCS or DECT networks, obtaining a limited set of UMTS services, due to the absence of the UMTS air-interface.
  This level corresponds to level 3 of ETR 0104 but without introduction of the UMTS air-interface [8].
- In the second evolutionary step (ASPeCT level 2 to ASPeCT level 3) the UMTS air-interface (Base Station Subsystem) is introduced. This also has implications on the core network (MSC/VLR) which must be capable of handling the new A-interface and mobility management procedures.
  ASPeCT level 3 corresponds to level 3 of the ETR 0104.
- In the fourth and last evolutionary step (ASPeCT level 3 to ASPeCT level 4), "full" UMTS services and features are provided, either via a further evolved GSM/DECT operator infrastructure or via a UMTS target network infrastructure utilising B-ISDN as backbone network. The main modifications are in the core network which will be able to offer all the UMTS services and features.

In the following, the above identified migration steps will be described in terms of:

- the mobile equipment types (single-mode, dual-mode, multi-mode) that might operate in conjunction with the SIM types (single-application, multi-application) that they may accept,
- the supported access systems (GSM, GSM/DCS, GSM/DCS/DECT, UMTS, etc.),
- the core network characteristics (functionality, interfaces, protocols, etc.),
- (user) roaming related aspects and
- services and features that could be offered (based on the overall network configuration).

Note that security related aspects will not be discussed in this section, since the aim here is to describe the evolution of the GSM network infrastructure towards UMTS. 'Security migration' will be tackled in the following sections. In fact, security related aspects need to be investigated at each "transition phase", as described in section 3.

[8] The "access" of the UMTS users is attained via the GSM900, DCS1800 and DECT access systems since UMTS BSSs haven't been installed yet. Therefore, high bit rate services (up to 2 Mbits/sec) are not available.

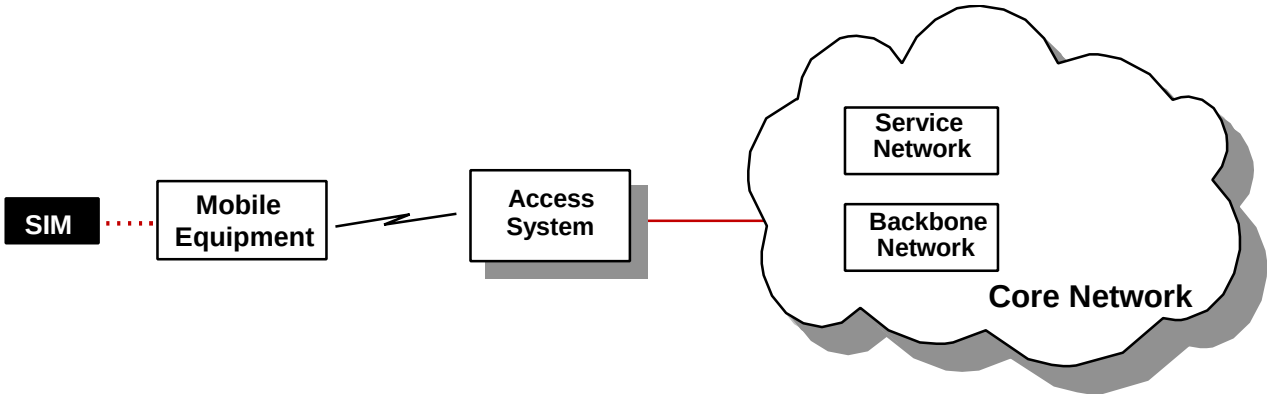


Figure 4-1: Entities Involved in the Migration Process

4.1 ASPeCT level 1 : Initial Network Level

A GSM operator utilising the same core network infrastructure serves GSM900, DCS1800 and DECT mobile users, offering mobile services to both private and public environments (Figure 4-2)[9]. The support of DCS1800 over an "existing GSM900 infrastructure" affects mainly the functionality of the GSM BSC (increased signalling load, frequency allocation, faster handover execution times, etc.), while DECT 'acts' as a BSS (Base Station Subsystem) [4] allowing the GSM MSC/VLR to 'see' DECT users as GSM users. From the GSM fixed network point of view, the DECT subscriber is a GSM subscriber i.e., the data structures and functionality in the GSM network are standard GSM (e.g., IMSI's), but instead of using a GSM air-interface as an access method to the GSM PLMN, the DECT CI is used instead [4].
The only extra requirement for a DECT PP compared to the standard Public Access Profile (PAP) portable for incoming calls is the ability to calculate the response to an authentication challenge with the standard GSM algorithm and, derive the DECT ciphering key from the calculated GSM key with the standard DECT algorithm [4].
On the other hand, the provision of IN-services introduces certain requirements in the GSM MSC/VLR (support of new protocols, increased signalling load, etc.), the functionality of which should be upgraded to GSM Ph2+ MSC/VLR. Note that at this stage, it will be given the possibility to mobile users to utilise GSM services via fixed terminals using their SIM.
The basic features of the "initial network level" are described below :

Access System
Access to the GSM/DCS services is supported via GSM Ph2+ BTSs, DCS Ph2+ BTSs and GSM Ph2+ BSCs, supporting also DCS functionality. GSM and DCS Ph2+ BTSs are attached to the same Ph2+ BSC. The GSM Ph2+ BSC is interconnected to the GSM Ph2+ MSC/VLR via the A-interface. DECT access is supported via DECT Fixed Parts (FP). DECT FPs are interconnected to GSM Ph2+ MSC/VLR(s) either via an IWU (through a DSS.1 interface extended with the A-interface protocol) or via a PBX.

Core Network
The MSC/VLR functionality is upgraded to Ph2+ MSC/VLR to enable interworking with the IN-SCP functionality which has been added to the network (see GSM-SCP network component).
The Ph2+ MSC/VLR is connected to the GSM-SCP via the CAMEL[10]/CS-2 interface [1].
The Ph2+ HLR/AC/EIR is attached to the Ph2+ MSC/VLR via the MAP-interface.

SIM
The envisaged SIM types for the initial network level are:

[9] In Figure 2 the symbol "/" corresponds to the term "and/or".

[10] The CAMEL feature provides the mechanisms to support services of operators which are not covered by standardised GSM services even when roaming outside the Home PLMN. CAMEL type services will emphasise on-line charging features like access to accounting information and credit control.

- GSM SIM
- DCS SIM
- DECT SIM
- Multi-application SIMs: GSM/DCS/DECT SIMs.

Note: GSM/DCS/DECT SIMs could be used as a UPT-like card.

Terminal Equipment

The envisaged terminal types are:

- Single-mode GSM terminals with 900 MHz radio interface (may accept DCS SIM).
- Single-mode DCS terminals with 1800 MHz radio interface (may accept GSM SIM).
- Single-mode DECT terminals (portable parts (PP)) allowing GSM/DCS users to register on using their GSM/DCS SIM.
- Multi-mode terminals with GSM/DCS/DECT access capabilities will accept all the available SIM types.

Roaming Aspects

The GSM Ph2+/DECT system will support roaming between DECT subsystems and GSM backbone network. It will be given the possibility to GSM/DCS users to utilise DECT terminals via GSM/DCS SIMs. GSM, DCS and DECT users may be registered on fixed terminals utilising both mobile and fixed network services.

Services & Features

The main teleservices of Level 1 GSM are: telephony, emergency calls, alternate speech and facsimile group 3, automatic facsimile group 3, short message service (mobile originated, mobile terminated, cell broadcast). Provision of teletex and videotex is possible when needed.
The different bearer services of Level 1 GSM cover bit rates from 300 to 9600 bps.
Level 1 GSM provides versatile supplementary services including multi-party call, calling line identification presentation/restriction, call waiting, call hold, call transfer and a range of different call forwarding and barring services.
Level 1 GSM provides multiband operation by single operator (same BSC and MSC for both GSM and DCS BTSs) and same user access (SIM) to both GSM and DCS terminals.
The supplementary services provided consist of GSM Phase 2 and CS-1 supplementary services. Voice mail box and TCP/IP support for data services are additional features provided but not standardised within the GSM standard.

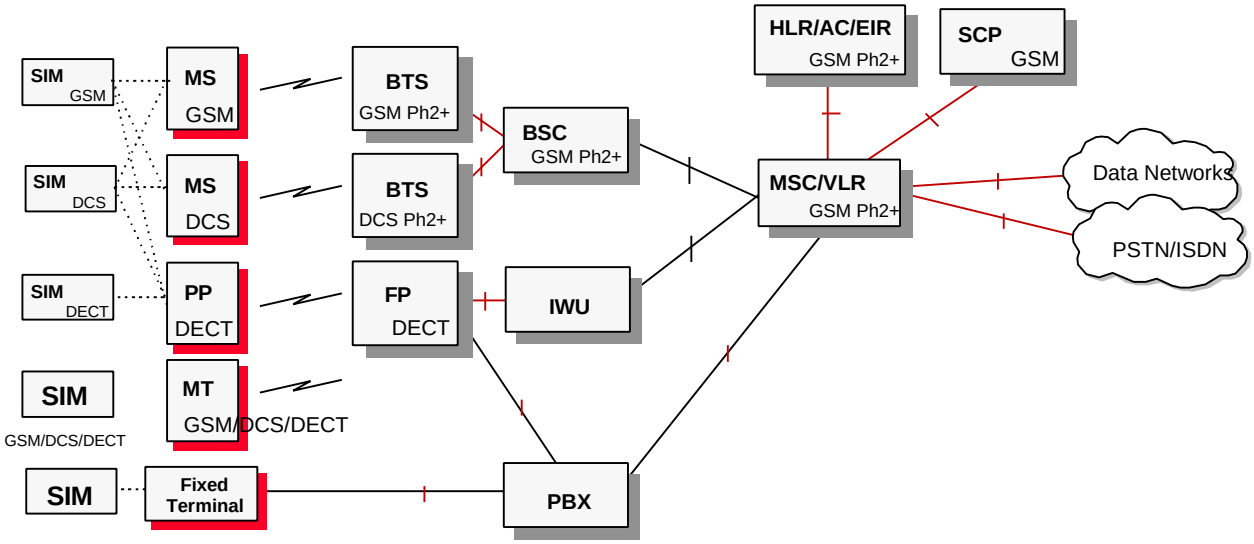


Figure 4-2 : ASPeCT level 1: The "Initial Network Level"

4.2 ASPeCT level 2 : Introduction of UMTS Users

At this level, the previous level GSM/DECT operator functionality will be enhanced so as to support **also** roaming of UMTS users[11] in GSM/DCS and DECT systems (Figure 4-3)[12]. This will be achieved by the introduction of advanced IN-functionality, located in the UMTS-SCP network component. However, a limited set of UMTS services will be offered at this level, due to the absence of the UMTS air interface. For example, high bit rate services will not be available.
The UMTS SIM (or UIM) will be introduced at this level.
The basic features of this level are described below:

Access System
There are no modifications in the access system.

Core Network
New modified HLR/AC/EIR and a combined CAMEL/CS-3 subset for SCP access.
The interface between HLR/AC/EIR and SCP might be useful for certain applications. The HLR/AC/EIR may also act as an interworking unit between a Phase 2+ GSM MSC/VLR and a UMTS SCP using a proprietary interface between the HLR/AC/EIR and the SCP.

SIM
The envisaged SIM types for this level are:

- GSM SIM
- DCS SIM
- DECT SIM
- UMTS UIM/SIM: A new UIM which offers full UMTS services in a real (planned or existing) UMTS network and part of the UMTS services in a GSM/DCS/DECT network.

Multi-application UIM/SIMs: GSM/DCS/DECT/UMTS UIM/SIMs.
Note: GSM/DCS/UMTS SIMs/UIMs could be inserted to a DECT PP and possibly to a fixed terminal as a UPT card.

Terminal Equipment
The envisaged terminal types are:

- Single-mode GSM terminals with 900 MHz radio interface.
- Single-mode DCS terminals with 1800 MHz radio interface.
- Single-mode DECT PPs allowing DECT users to access DECT services.
- Dual-mode terminals providing GSM/DCS and DECT access, will support all the available SIM types.
- Pre-UMTS terminals with a GSM/DCS or DECT air-interface and UMTS smart card interface may be useful.

Note: Single-mode terminals will probably accept more than one SIM type.

Roaming Aspects
The GSM/DECT system will support roaming between DECT subsystems and GSM backbone network. It will be given the possibility to GSM/DCS users to use DECT terminals using their GSM/DCS SIM. UMTS users will be able to utilise UMTS services as well as to roam in GSM/DCS/DECT systems, using their multi-mode SIM and the appropriate terminal type. It is likely that UPT-like services will be offered to mobile users by registering themselves to fixed terminals using their SIM.

Services & Features
A limited set of UMTS services and features will be offered with modification of the SIM/UIM and the GSM-UMTS SCP or HLR/AC/EIR.

---

[11] Users having a UMTS subscription with a UMTS service provider.

[12] In Figure 3 the symbol "/" corresponds to the term "and/or".

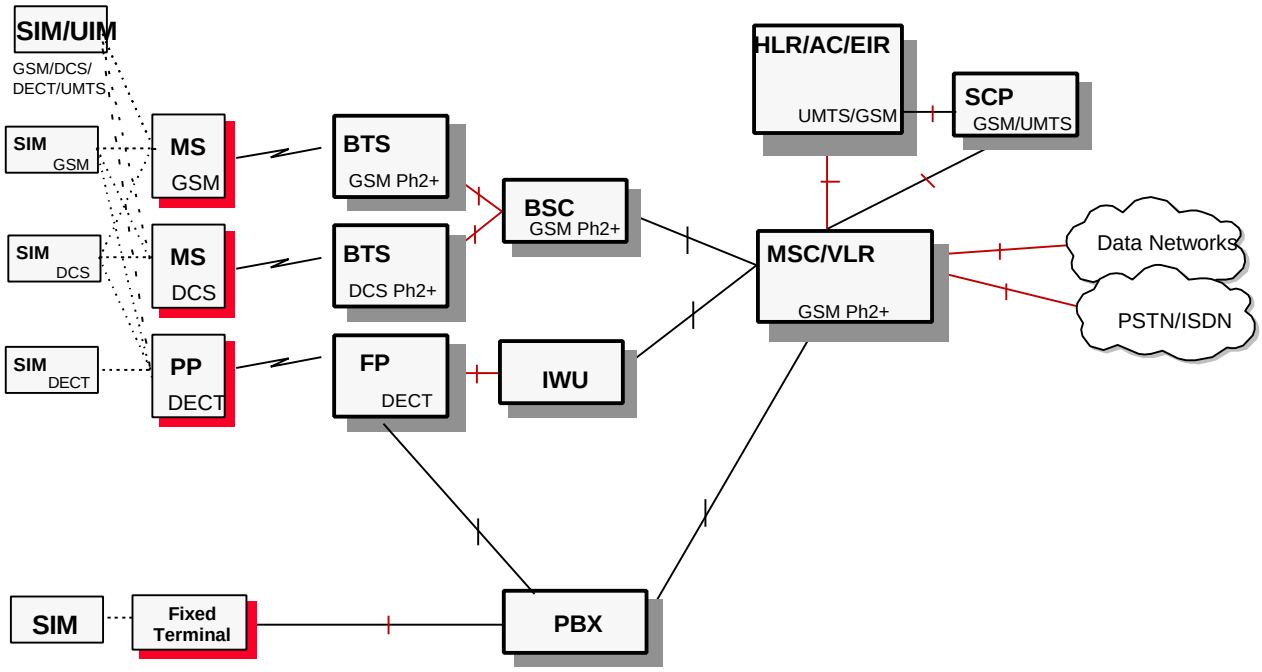


Figure 4-3: ASPeCT level 2 - Support of UMTS Users Roaming over Ph2+ GSM Network Infrastructure

4.3 ASPeCT level 3 : Introduction of UMTS Air-interface

At this level the UMTS air-interface is introduced. A subset of the UMTS services will be supported at this level mainly due to the limitations imposed by the GSM fixed network infrastructure. The basic features of this level are described below:

Access System

New UMTS base station subsystem which supports terrestrial UMTS radio interface(s). The access to MSC is realised by a new modified interface. The interface might support the use of ATM.

Core Network

Upgrade of the GSM MSC/VLR to a UMTS MSC/VLR to support the UMTS A-interface to the UMTS BSS. The supported mobility management procedures are an evolution from the mobility management procedures of GSM Phase 2+.

SIM

The multi-application UMTS UIM is extended with new services and features that can be offered due to the introduction of the UMTS air-interface.

Terminal Equipment

The envisaged terminal types are:

- Single-mode GSM terminals with 900 MHz radio interface.
- Single-mode DCS terminals with 1800 MHz radio interface.
- Single-mode DECT PPs allowing DECT users to access DECT services.
- Dual-mode terminals providing GSM/DCS and DECT access, will support all the available SIM types.
- Multi-mode UMTS terminals with a GSM/DCS/DECT and UMTS air-interface -allowing the support of various SIM/UIM types.

Note: Single-mode terminals will probably accept more than one SIM/UIM type.

Roaming Aspects

The GSM/DECT system will support roaming between DECT subsystems and GSM backbone network. It will be given the possibility to GSM/DCS users to use DECT terminals using their GSM/DCS SIM. UMTS users will be able to utilise UMTS services as well as to roam in GSM/DCS/DECT systems either using their multi-mode SIM/UIM or using the appropriate terminal type. It is likely that UPT-like services will be offered to mobile users by registering themselves to fixed terminals using their SIM.

Services & Features

ASPeCT level 3 will support part of the services (such as multimedia and videotelephony) planned for UMTS. The first parts of UMTS standards will incorporate the features of the preceding levels. SIM as well as terminal roaming is supported between GSM/DCS and UMTS.

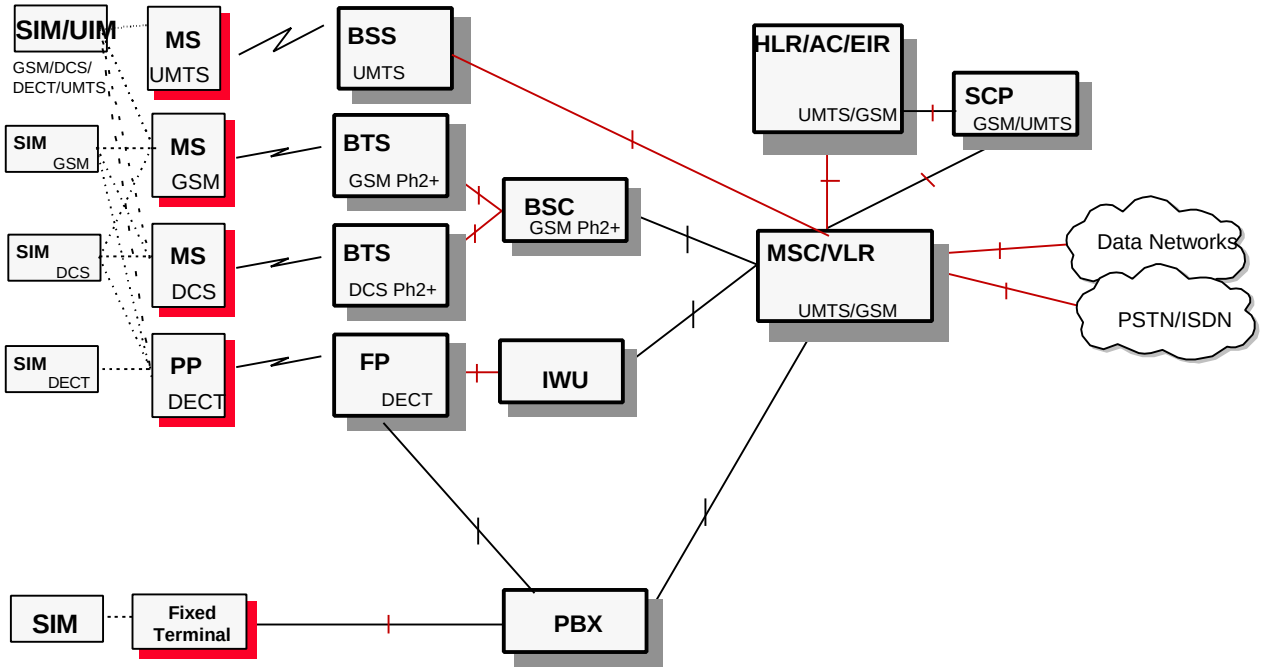


Figure 4-4: ASPeCT level 3 : introduction of UMTS air-interface

4.4 ASPeCT level 4 : UMTS system, evolved from GSM

ASPeCT level 4 will provide the full set of UMTS services including the broadband (up to 2 Mbits/s) services via the UMTS radio interface to limited coverage areas. ASPeCT level 4 UMTS systems will fulfil all UMTS requirements and is depicted in Figure 4-5.
The basic features of the level 4 are described below:

Access System

There are no modifications in the access system.

Core Network

It is unclear which architecture the core network will have. The core network may support ATM switching.

SIM

The envisaged SIM types are:

- GSM SIM
- DCS SIM
- DECT SIM

- UMTS UIM
- Multi-application UIM/SIMs: GSM/DCS/DECT/UMTS UIM/SIMs.

Note: GSM/DCS/DECT/UMTS SIMs will be possibly used as UPT cards.

Terminal Equipment

The envisaged terminal types are:

- Single-mode GSM terminals with 900 MHz radio interface.
- Single-mode DCS terminals with 1800 MHz radio interface.
- Single-mode DECT PPs allowing DECT users to use DECT services.
- Single-mode UMTS Mobile Terminals (MT) allowing UMTS users to access UMTS BSSs.
- Adaptive multi-mode terminals combining UMTS, GSM/DCS and DECT access technologies - allowing support of various SIM/UIM types.

Note: Single-mode terminals will probably accept more than one SIM/UIM type.

Roaming Aspects

Visited networks may offer additional services to roaming UMTS users, due to the new UMTS radio interface.

Services & Features

ASPeCT level 4 offers "full" UMTS services and features.

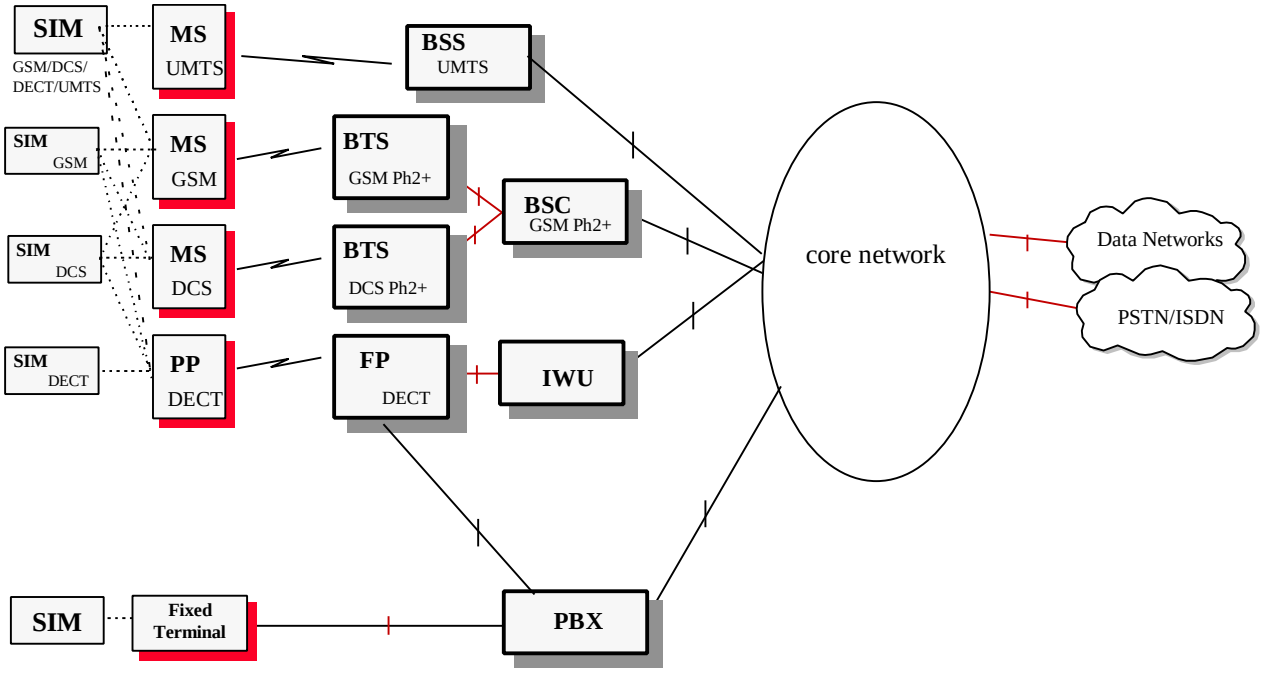


Figure 4-5: ASPeCT level 4 - Full UMTS

5. Introduction to the framework for authentication

This section will introduce the concept of an authentication framework and explain its advantages in support of migration towards UMTS. Key points considered will include the concept of user *capability classes*, user-network (mutual) authentication using *negotiated mechanisms*, and the establishment of NO - SP *automatic roaming agreement*.

This section contains :-

- The objectives of the framework
- The framework's requests and procedures
- General issues regarding the framework
- Framework interface definitions

5.1 Objectives of the framework

5.1.1 To provide a flexible procedure for user-network authentication

The principle objective of the framework is to define a set of procedures for UMTS whereby user-network authentication can be implemented in a flexible way, allowing a number of different mechanisms and algorithms to be incorporated, with the ability to migrate smoothly from one mechanism to another.
The framework would allow the authentication capabilities of users, network operators and service providers to be taken into consideration when agreeing a mechanism to use. A list of acceptable mechanisms will need to be maintained so that different entities can identify and implement the mechanisms they require.

5.1.2 To provide a procedure for SP-NO roaming agreement

In UMTS a large number of network operators and service providers will exist. In order to facilitate roaming it may be necessary (or just desirable) for roaming agreements to be set up dynamically, as and when they are required. In practice the roaming agreement would be first requested as part of an initial authentication request sent by the user to a new network operator. A prerequisite of this procedure is that the SP and NO who wish to establish the agreement have authenticated each other.

5.1.3 To provide a procedure for SP-NO authentication

NO-SP authentication will be carried out using a globally agreed mechanism in order to ensure that NOs and SPs world-wide have the capability to authenticate each other. Unlike the user-network authentication mechanism, flexibility to change mechanisms is not considered to be a crucial factor.
Apart from being a prerequisite to a roaming agreement, NO-SP authentication will permit the SP to delegate user-network authentication to the NO. The SP would send authentication data to the NO in advance, permitting the NO to carry out authentication on behalf of the SP.

5.2 The proposed authentication framework

5.2.1 Authentication framework requests

Scenarios that involve the authentication framework fit into two main categories: those that involve a request for user-network authentication, and those that involve a request to establish a NO-SP roaming agreement. A request may involve all or some of the authentication framework procedures, outlined in Section 5.2.2.

5.2.1.1 Request R1: User authentication request

A user authentication request is defined as a request from network to user, or vice-versa, to perform user-network authentication. The requesting network entity may be the NO or the SP. Authentication requests may involve all authentication framework procedures, as outlined in Section 5.2.2, which may include a roaming agreement request. An authentication request is invoked whenever user-network authentication is to be performed.

5.2.1.2 Request R2: Roaming agreement request

A roaming agreement request is defined as a request from SP to NO, or vice-versa, to establish a roaming agreement. Roaming agreement requests only use authentication framework procedures P3 and P4, as outlined in Section 5.2.2. A roaming agreement request is invoked whenever an NO or an SP wishes to allow the SP's users to roam onto the NO's network according to certain negotiated conditions.

5.2.2 Authentication framework procedures

5.2.2.1 Procedure P1: User - NO authentication capability agreement

User and NO inform each other of their respective authentication capabilities, and subsequently agree the mechanisms to be used during their interaction. Exchanges will not include the user's identity, instead an *authentication capability class* indicator would be sent. Note that the user's identity is not sent at this stage, since any establishment of a roaming agreement and identification of a user's authentication Capability Class do not require that the visited NO knows the identity of the user. The authentication capability class would be used to categorise users according to their capabilities regarding user-network authentication. A particular class would identify a large collection of users having the same authentication capabilities: they might have the same version of UIM, for example. In practice, the authentication capability class may also identify the user's SP, or the SP may be identified in a separate message from the user to the visited NO.
On receiving the user's authentication capability class and Service Provider Identity, the NO checks to see if it has previously decided on an authentication mechanism to be performed with users in that particular class and belonging to that particular Service Provider. Negotiation with that particular Service Provider will be necessary, even if the capability classes are standardised, in order to allow the Service Provider to request a preferred mechanism from the supported mechanisms, as described in Section 2.2.2. If a mechanism has not been decided on, then the NO must negotiate with the user's SP by executing P2, as described below.
Once the SP and NO have agreed a mechanism for use with users in a particular authentication capability class, the NO will instruct the user to perform the agreed mechanism. This instruction may be signed by the SP as well as the NO, in order to confirm to the user that both the SP and the NO have agreed to the instruction.
In the eventuality that the user does not have a certificate to permit it to validate the NO signature of an authentication mechanism prescribed to it, it will still have the assurance that the mechanism has been approved by the SP, by virtue of the SP's signature.

5.2.2.2 Procedure P2: NO-SP authentication capability agreement

SP and NO interact in order to negotiate the user-network authentication mechanism to be used, based on the capabilities and preferences of the entities involved. Specifically, the NO requests information from the user's SP to identify the authentication capabilities possessed by the user, according to his authentication capability class. The SP will respond with the user's authentication capabilities and may also send signed instructions to the NO to request the use of a preferred mechanism. On receiving this information the NO will make a decision based on the capabilities and preferences, before sending the identity of the prescribed mechanism to the user.

5.2.2.3 Procedure P3: Service provider - network operator authentication

SP and NO interact to authenticate each other. A globally accepted standard specification must be followed. A suitable candidate might be the ITU X.509 certificate-based authentication procedures. The emergence of widely acceptable underlying algorithms has not yet occurred, but a global certification hierarchy (based on TTPs) is emerging. Any 'registered' (hash-appendix type) signature scheme can be used (including RSA, DSS, El-Gamal) with X.509.

5.2.2.4 Procedure P4: Establishment of NO - SP roaming agreement

NO or SP initiate a procedure to establish a roaming agreement. This may be done on-line as part of an authentication request in a registration attempt, or off-line as a separate procedure. A roaming agreement may have to be established, modified or terminated, and appropriate procedures should exist for each of these cases. Off-line agreement may be done by physically passing messages in a secure manner using cryptographic or non-cryptographic techniques. On-line agreement, on the other hand, can only be done in practice using cryptographic techniques.

This procedure deals primarily with on-line establishment of roaming agreements using cryptographic techniques only, since this is considered to be an integral part of the authentication framework. However, the procedures may also be a basis for off-line establishment of roaming agreements using cryptographic techniques, which may turn out to be a more important case.

The number of messages required and their respective contents is for further study, as is the length of validity for the roaming agreement, its modification and its revocation. Typically, the exchanged messages will require origin authentication, non-repudiation, integrity and confidentiality which will, like the SP-NO authentication, require globally acceptable standardised mechanisms.

5.2.2.5 Procedure P5: User - network authentication

The user and network interact to authenticate each other. This procedure should allow requests from network to user, or vice-versa, to perform user-network authentication. The requesting network entity may be the NO or the SP.

Delegation of user-network authentication to the NO is likely to be required in UMTS in order to reduce the signalling requirements between NO and SP, such that authentication data need only be sent to the NO as part of each new registration[13]. However, since it is the SP that stores the user-related information, the SP must have some involvement in the mechanism, if only to pass or register authentication data with the NO in order to let the NO perform authentication on the SP's behalf, or to delegate (off line) the authority to perform authentications to an approved Certification Authority (CA). Therefore, depending upon the particular authentication mechanism to be employed for new registrations, either the SP will have a direct interaction with the visited NO, or a CA approved by the SP will act as an authentication proxy on behalf of the SP. Note that in any case, for new registrations, the SP will *always* be contacted by the visited NO for the purposes of Location Registration, so that calls may be routed to the visited NO, and also that a definition of the respective authentication Capability Class may be passed from the SP to the visited NO (refer to Section 5.2.2.2).

Two main instances of the user-network authentication procedure exist depending on whether or not the SP (or a CA) is involved. If the user is not currently registered, then the *authentication mechanism for new registrations* (P5a) is performed. This will involve a request for authentication data from the SP (or a CA). If the user is currently registered, then the *authentication mechanism for current registrations* (P5b) is performed. This may not involve the SP (or a CA).

The framework will allow the 'soft' migration of user-network authentication mechanisms, where each entity may be capable of performing more than one mechanism in order to facilitate a smooth and gradual phased transition to a new mechanism. This is preferable to a 'hard' migration, where all entities must be updated with the new mechanism at once, which would result in a one-step migration path.

Once the user and network have agreed an authentication mechanism to use by executing procedures P1 and P2, the authentication itself can begin. This will involve exchanges between the user and NO, and between the NO and the SP (or a CA) for new registrations. In addition, exchanges between the NO and the SP may be required for current registrations depending whether or not authentication data is required. The exchanges for new registrations may also involve interaction with one or more Certification Authorities.

[13] Strictly, this may not be the case since the authentication data may only permit a finite number of user-network authentications, then the NO may be required to send requests to the SP during a current registration, as is the case with GSM security triplets.

5.3 General issues regarding the framework

5.3.1 Standardisation

Apart from the underlying user-network authentication mechanism itself, the framework should be completely standardised. Therefore, a list of acceptable user-network authentication mechanisms needs to be maintained. Unlike the user-network authentication procedure which must be flexible, a single mechanism for SP-NO authentication should be standardised. By using a single mechanism, the flexibility for future enhancement is reduced. However, the ability to update the user-network authentication mechanism efficiently is far more important since it involves the use of a critical resource; the radio interface. Future enhancements to the user-network authentication mechanism may comprise minor changes to give faster or more easily implemented mechanisms, which is perhaps not worth doing in the less critical NO-SP authentication.
What constitutes an 'acceptable' user-network authentication mechanism also requires consideration. Allowing unrestricted use of any (service provider defined) mechanism is unacceptable since problems may occur when a network operator deems a service provider's mechanism to be unacceptable. Thus some form of quality control and perceived acceptability, such as registration of mechanisms, is required. This could be managed by a responsible body acting as a TTP. Acceptable mechanisms will temporarily include certain Second Generation mechanisms (GSM, DECT, UPT etc.), and could also include parameterised families of mechanisms to allow some service provider choice.

5.3.2 Modularity

The desire for subsystem independence should extend to all levels of UMTS, in particular the separation of security into independent procedures. For example, it should be possible to modify or replace the roaming agreement procedure, or SP-NO authentication, without impacting (to a serious degree) on any other procedure. In view of this, a modular approach is adopted whereby five separate procedures are specified and may be combined in various ways to form application-dependent procedures.
Adopting a modular approach has its drawbacks. It means that to support the necessary interactions between modules, standardised interfaces are required, which imposes a set of conformance requirements. These issues are dealt with further in Section 4.

5.3.3 User independence

An important feature of the framework is that the procedures to be carried out prior to user-network authentication are essentially independent of the user's identity. This is done by using an authentication capability class to identify users according to their authentication capabilities. The independence from the user's identity permits the use of various strategies for providing user identity confidentiality through different user-network authentication mechanisms using either temporary or encrypted identities.

5.3.4 Access interface agreement

In UMTS, it is likely that network operators will employ different access interfaces. Therefore to provide full inter-network roaming the network and mobile equipment will have to agree on a suitable access interface. This may involve the downloading of the appropriate capabilities to the mobile equipment over a fairly basic air interface.
Access interface agreement, if implemented, will probably have to follow the authentication process, because it relies on a trustworthy link between the mobile equipment and the network. Therefore, a basic interface must exist, or be initially agreed, which will be capable of supporting the authentication process.

5.3.5 Inter-operator handover

It is not yet clear whether inter-operator handover will exist in UMTS, or whether direct interaction is required between operators for any other reason (e.g. 'seamless roaming').
All procedures identified in Section 5.2.2 will remain valid if the SP is replaced by a second NO. The interpretation of procedures will change accordingly. For example, P4, the NO-SP roaming agreement procedure, would become a 'NO-NO handover agreement procedure'.

5.3.6 Service provision

Service provision is separate from, and must come after, authentication. Some of the necessary exchanges in the service provision procedure could occur within the authentication framework procedures. Nevertheless, modularity of subsystems (e.g. security, mobility, service provision, etc.) is a key objective in UMTS, to give flexibility. This motivates the separation of security aspects from other UMTS procedures like registration or service provision.
In practice, service provision will be interrupted by the authentication process. The service request will precede authentication, but the service provision activities will follow the authentication[14].

5.4 Authentication framework interface definitions

5.4.1 Interaction with other UMTS subsystems

5.4.1.1 User-network authentication and encryption mechanism

Perhaps the single most important interface between subsystems is that between the user - network authentication procedure (more specifically the session key generation) and the 'encryption mechanism'. Clearly the key generation mechanism must be flexible enough to supply a suitable key irrespective of the encryption mechanism. That is, it must be able to generate a key of variable length[15].

5.4.1.2 User-network authentication and user identity confidentiality mechanism

Another interface requiring consideration is that between the user identity confidentiality mechanism and other (non-security) procedures involving the user identity. The procedures must be compatible in that they must use the same form of identity.

5.4.2 Conformance requirements

In practice the user authentication, user identity confidentiality and session key generation are usually carried out concurrently - the first two by necessity and the third for convenience. This is likely to remain the case for UMTS. Therefore none will be entirely standardised.

In view of this we may be required to ensure all parameters (identities, keys etc.) generated, modified or utilised during the authentication processes conform to requirements imposed by other system procedures.

[14] Except in special cases where authentication may not be performed (e.g. permitting emergency calls with no UIM)

[15] This leads to the separate, but related question as to whether an architecture for encryption should be standardised, and where the functionality to support this at the user end should be placed (may be in the ME, the UIM or both). Furthermore, the issue of whether end-to-end encryption should be implemented as an integral part of UMTS still exists.

6. Functional description of GSM phase 2+ security

The work items of phase 2+, currently defining impact on security are summarised, enhanced with work items, for which security impact has been defined in the ETSI STC SMG10.

An overview is given of the interfaces and protocols relevant to security in GSM phase 2. A relevant message flow, summarising the GSM security procedures is described.

6.1 Security Features in GSM phase 2

GSM security features are standardized in GSM 02.09 [5].

The following security features are considered :

- subscriber identity (IMSI) confidentiality
- subscriber identity (IMSI) authentication
- user data confidentiality on physical connections
- connectionless user data confidentiality
- signalling information element confidentiality

A detailed description of the mechanisms that support these features can be found in the ASPeCT deliverable D2 [6], sections 7.2.1.1 to 7.2.1.3.

6.2 Phase 2+ Work Items with impact on security

Some of the work items of phase 2+ define impact for security :

6.2.1 Payphone services

A service whereby a user not having any GSM subscription can make use of GSM services using coins, SIM card, credit card or prepaid cards.

Security Aspects:
The following security mechanisms are necessary:
- payphone SIM to network authentication,
- network to payphone SIM authentication,
- transferred data and payphone SIM stored data integrity certification,
- non repudiation

Stage 1 document due SMG Meeting #23

6.2.2 Transparently supporting UPT phase 1

This work item contains a feasibility study on how GSM PLMN's can support UPT phase 1.

Security Aspects:
A UPT user has to "borrow" a GSM ME and SIM to access the GSM PLMN. The owner of the MS may want to bar calls to other numbers than the one related to the UPT service.
This service may be an additional work item.

Work Item is under study, SMG1 reported that no work is required.

6.2.3 Inter operation with UPT phase 2

The UPT service allows UPT users to make calls from and receive calls in any network. This work item allows UPT users to have access from GSM networks, using UPT smart cards.

Security Aspects:

Compatibility with a new smart card, will involve investigation of:
- authentication,
- identification,
- encryption,
- signalling interworking,
- others.

No status can be found.

6.2.4 user to user signalling

A service which allows to send messages directly from one user to another. The difference with SMS is that there is no store-and-forward centre, no delay.

Security Aspects:
The UUS message will be encrypted using the same algorithm as for speech..
Status : stage 1 complete

6.2.5 IMEI check digits

When an IMEI is being reported by humans (e.g. by speech or typing) there is significant chance of errors being made, which might be serious if they result in the blocking, or unblocking, of the wrong MS in an EIR.

Security Aspects:
The GSM MoU is expected to define a suitable algorithm (not required to be implemented in the MS) for specifying the check digits. It is thought that error detection is adequate, without the need for error correction.

No status can be found ??

6.2.6 Mutual Authentication

There are a number of applications where it is necessary for the SIM to perform a mutual authentication with an entity in, or connected to, the network. An example would be for home banking.

Security Aspects:
Secure mutual authentication is required.

Requirements are due at SMG Meeting #20.

6.2.7 IMEI Security enhancements

A certificate principle is proposed. The authenticity of IMEIs can be checked. This mechanism is not protecting against duplication of IMEIs. It was mentioned that this mechanism is a step forwards for IMEI protection, and was presented for information and consideration. Efforts from manufacturers are required to improve physical security. The type approval authorities are not able to check the secure storage in the ME of the IMEI.
The proposed procedure on IMEI security enhancements was not supported by the SMG Meeting 19 and will not be implemented by SMG. The work on this topic is stopped.

6.2.8 High Speed Circuit Switched Data

Data service based on use of up to eight time slots per TDMA frame. Both transparent and non-transparent services should be supported.

Security Aspects:
The same security is required as for other bearer services.

Due date for ETR was SMG Meeting #19, some delay occurred.

6.2.9 General Packet Radio Services

Proposals for GPRS encryption were analysed by the security group of SMG. The proposed encryption mechanisms (provide encryption between the MS and the SGSN, Serving GPRS support node) were considered to require more study and co-operation with the network group of SMG.

6.2.10 SIM application toolkit

The security group of SMG believes that more security features are needed. Therefore a joint working party, between the security group and the smartcard group, “SIM Toolkit Security” has been established. A feasibility study on security features for the transport of messages between the HPLMN and the SIM has been started.

6.3 Overview of the interfaces and protocols relevant to security

Interfaces are defined in GSM between the following entities :

- SIM
- Terminal (MS)
- BTS
- BSC
- MSC
- VLR
- The integrated entity HLR and AC

Figure 6-1 illustrates a GSM networks with its entities.

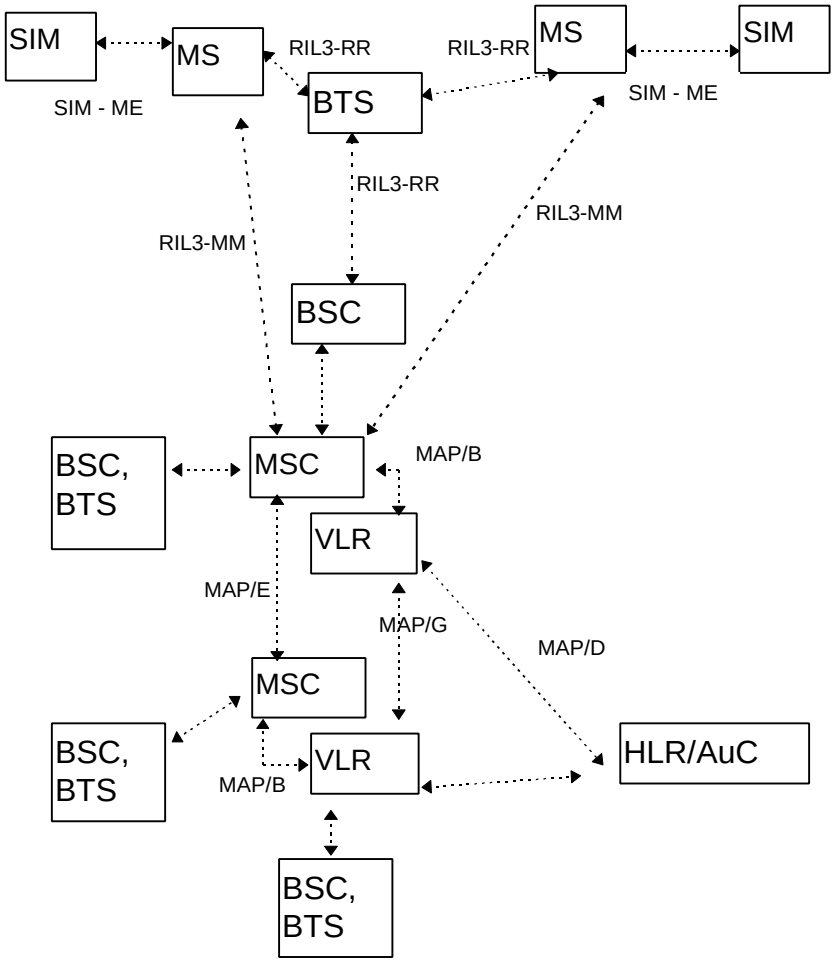


Figure 6-1 : GSM before start of the migration/evolution

Below a description of the interfaces with a list of security relevant messages or commands (in case of SIM-ME interface) with an indication of the GSM recommendations where the message is described.

RIL3 - MM (GSM 04.08) [7]

The RIL3-MM protocol connects the MS to the MSC (Radio Interface Layer 3, Mobility Management). It uses the MS-MSC signaling connection provided by the RR layer. It also supports Security and Mobility Management functions.

AUTHENTICATION REQUEST
AUTHENTICATION RESPONSE
AUTHENTICATION REJECT
IDENTITY REQUEST (When the network does not know the TMSI it will request the IMSI)
IDENTITY RESPONSE
TMSI REALLOCATION COMMAND
TMSI REALLOCATION COMPLETE
LOCATION UPDATE REQUEST (May include the TMSI or IMSI)
LOCATION UPDATING ACCEPT (When the TMSI allocation is performed just after a successful location update, the TMSI is included in this message and the TMSI REALLOCATION COMMAND is not sent)

SIM - ME (GSM 11.11) [8]

This is the interface between the SIM and the mobile station

RUN GSM ALGORITHM (request to calculate Kc and SRES + contains RAND)
GET RESPONSE (response to GET RESPONSE = messages with Kc and SRES)

MAP/D (GSM 09.02) [9]

This is the interface between the visited VLR and the home HLR.
Phase 1
SEND PARAMETERS (VLR requests authentication info to the HLR)
SEND PARAMETERS RESULT
Phase 2
SEND AUTHENTICATION INFO (VLR requests authentication info to the HLR)

MAP/G (GSM 09.02) [9]

This is the interface between two VLR's
Phase 1
SEND PARAMETERS (VLR requests authentication info and IMSI to the previous VLR)
SEND PARAMETERS RESULT
Phase 2
SEND IDENTIFICATION (VLR requests authentication info and IMSI to the previous VLR)

RIL3 - RR (GSM 04.08) [7]

This is the interface between the BSC and BTS and between the BTS and mobile station.

CIPHERING MODE COMMAND (from BSC to MS via BTS)
CIPHERING MODE COMPLETE (from MS to BSC via BTS)
ENCRYPTION COMMAND (from BSC to BTS)

The BSSMAP CIPHER MODE COMMAND message indicates the new requested mode. After having extracted the new parameters from this message, the BSC builds up an RIL3-RR CIPHERING MODE COMMAND message targeted at the mobile station and encapsulates it in an GSM ENCRYPTION COMMAND message sent to the BTS. The BTS then configures its reception to the new mode and sends the encapsulated RIL3-RR CIPHERING MODE COMMAND message to the mobile station using the old mode.

When receiving it, the mobile station sets its configuration to the new mode and puts an RIL3-RR CIPHERING MODE COMPLETE message in the sending queue. This message will later be forwarded to the BSC, which translates it into a BSSMAP CIPHER MODE COMPLETE message to indicate to the MSC that its request has been fulfilled.

6.4 Message flows

6.4.1 Location Update with Authentication and TMSI Reallocation

The Message Flow illustrates a location update using TMSI in a new VLR-area. The previous VLR is requested for IMSI and authentication data. Only the IMSI is received, which means that a request for authentication data is sent to the HLR. A new TMSI is allocated by the new VLR and included in the location update accept message. Also a ciphering command is sent.

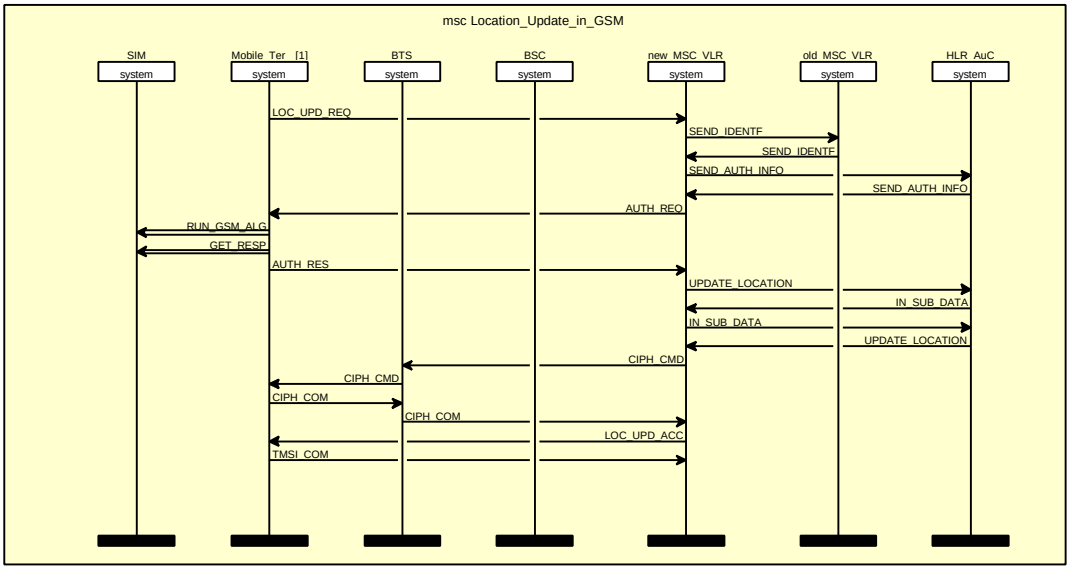


Figure 6-2 : Message flow : Authentication in GSM

6.4.2 Message contents

Only those information elements are given that are relevant to security. References to sections correspond to the sections in the referenced documents.

RIL3 - MM (GSM 04.08) [7]

AUTHENTICATION REQUEST (Section 9.2.2)
- Ciphering key sequence number (Section 10.5.1.2)
- Authentication parameter RAND (Section 10.5.3.1)

AUTHENTICATION RESPONSE (Section 9.2.3)
- Authentication parameter SRES (Section 10.5.3.2)

AUTHENTICATION REJECT (Section 9.2.1)

IDENTITY REQUEST (Section 9.2.10)
- Identity Type (Section 10.5.3.4)

IDENTITY RESPONSE (Section 9.2.11)
- Mobile Identity (Section 10.5.1.4)

TMSI REALLOCATION COMMAND (Section 9.2.17)
- Location area identification (Section 10.5.1.3)
- Mobile identity (Section 10.5.1.4)

TMSI REALLOCATION COMPLETE (Section 9.2.18)

LOCATION UPDATING REQUEST (9.2.15)
- Ciphering key sequence number (Section 10.5.1.2)
- Location area identification (Section 10.5.1.3)

Mobile identity (Section 10.5.1.4)
LOCATION UPDATING ACCEPT (Section 9.2.13)
Optional : Mobile Identity (Section 10.5.1.4)

SIM - ME (GSM 11.11) [8]

RUN GSM ALGORITHM (Section 9.2.16)
Command parameters/data : RAND
Response parameters/data : SRES, Cipher Key Kc
GET RESPONSE (Section 9.2.18)
Used to get the response parameters from RUN GSM ALGORITHM

MAP/D (GSM 09.02) [9]

SEND AUTHENTICATION INFO Request and Indication (Section 6.5.2)
IMSI
SEND AUTHENTICATION INFO Response and Confirmation (Section 6.5.2)
AuthenticationSetList : Rand, Sres and Kc

MAP/G (GSM 09.02) [9]

SEND IDENTIFICATION Request and Indication (Section 6.1.4)
TMSI
SEND IDENTIFICATION Response and Confirmation (Section 6.1.4)
IMSI, if known
Authentication Set, if available

RIL3 - RR (GSM 04.08) [7]

CIPHERING MODE COMMAND (Section 9.1.9)
Cipher Mode Setting (Section 10.5.2.9)
Cipher Response (Section 10.5.2.10)
CIPHERING MODE COMPLETE (Section 9.1.10)
Mobile Identity (Section 10.5.1.4). In this message the Mobile Identity will represent the Mobile Equipment Identity (IMEI)

6.4.3 Information elements

IMSI International Mobile Subscriber Identity [10]
A unique Mobile Subscriber Identity. The IMSI consists of three parts :
IMSI = MCC + MNC + MSIN
with
MCC = Mobile Country Code, 3 digits, administered by the CCITT.
MNC = Mobile Network Code, 2 digits, administered by the countries
MSIN = Mobile Subscriber Identification Number, administered by the operators
The maximum length of the IMSI is 15 digits

TMSI Temporary Mobile Subscriber Identity [10]
Allocated by the VLR. It has only significance in the area controlled by the VLR that allocated the number. It consists of 4 octets, the structure and coding of it can be chosen by agreement between operator and manufacturer in order to meet local needs.

IMEI International Mobile Equipment Identity [10]
Uniquely identifies a Mobile Station. It consists of 4 parts :
IMEI = TAC + FAC + SNR + spare
with
TAC = Type Approval Code, length 6 digits

FAC = Final Assembly Code, length 2 digits
SNR = Serial Number, length 6 digits
1 spare digit shall be zero when transmitted by the Mobile Station.

RAND The purpose of the Authentication Parameter RAND information element is to provide the mobile station with a non-predictable number to be used to calculate the authentication response signature SRES and the ciphering key Kc [11].
The length is 17 bytes :
byte 1 : authentication parameter RAND Information Element Identifier
byte 2-17 : Random value, consists of 128 bits. Bit 8 of octet 2 is the most significant bit while bit 1 of octet 17 is the least significant bit.

SRES The purpose of the authentication parameter SRES information element is to provide the network with the authentication response signature calculated in the mobile station [11].
The length is 5 bytes :
byte 1 : Authentication parameter SRES Information Element Identifier
byte 2-5 : The SRES value consists of 32 bits. Bit 8 of octet 2 is the most significant bit while bit 1 of octet 5 is the least significant bit.

Kc The ciphering key Kc is calculated by the Mobile Station and the Base Station ([6] and [11]).
The maximum length is 64 bits. Algorithm A8 which calculates Kc is operator specific. If the actual key produced by A8 is less than 64 bit then it will be extended into a 64 bit word where the non-significant bits are forced to zero. It is assumed that any non-significant bits are the least significant bits and that, the actual ciphering key is contained in the most significant bits.

Ki Individual Subscriber Authentication Key used to calculate Kc and SRES ([4] and [11]).
The key Ki is not prescribed by GSM but operator specific, together with the algorithms A3 and A8, used respectively to calculate SRES and Kc.

CKSN The purpose of the Ciphering Key Sequence Number information element is to make it possible for the network to identify the ciphering key Kc which is stored in the mobile station without invoking the authentication procedure. The ciphering key sequence number is allocated by the network and sent with the AUTHENTICATION REQUEST message to the mobile station where it is stored together with the calculated ciphering key Kc.
The length = 1 octet.
Bits 5-8 : Ciphering Key Sequence Number Information Element Identifier
Bit 4 : spare
Bits 3-1 = 1 1 1 means no key available
= other value is the sequence number

7. Functional description of UMTS security and of the framework for authentication

This section describes the target UMTS network status, after all transitional phases towards migration have occurred. The UMTS system is described in terms of the different operational scenarios.

Operational scenarios involving the Authentication Framework fit into two main categories: those that involve a request for user-network authentication, and those that involve a request to establish an NO-SP roaming agreement. Each type of request is dealt with in turn.
Message flow diagrams are given for each scenario. The terminology in Table 0-1 below is used to describe messages. Messages are categorised in the table according to the authentication framework procedure they belong to. A more detailed specification for typical user-network authentication mechanism(s) that can be incorporated within the framework, will be given for the Royal Holloway Symmetric Key Challenge-Response Mechanism [6] and/or the Siemens Public Key-Based Mechanism [6], refer to Chapter 10.

P1		
	InitAuthRqt	Initial authentication request (sent from user to NO). This includes a message identifier.
	InitAuthRqtNO	Initial authentication request (sent from NO to user). This includes a message identifier.
	InitAuthRqtSP	Initial authentication request (sent from SP to user)
P3		
	AuthRqtSPNO	Authentication request (SP-NO)
	AuthAckSPNO	Authentication acknowledgement (SP-NO)
P4		
	RoamRqt	Request to negotiate roaming agreement
	RoamAck	Acknowledgement that roaming agreement was negotiated (may be unsuccessful
P2		
	CapsRqt	Request for information on authentication capability class
	CapsInfo	Response information on authentication capability class enquiry
P1		
	PresAuthMech	Prescribed authentication mechanism
	AuthMechAck	Acknowledgement that the prescribed mechanism will be initiated
P5		
	AuthDataRqt	Request for authentication data
	AuthDataInfo	Response to authentication data request
	AuthDataRes	Result of user-network authentication

Table 7-1 Terminology used in the message flow diagrams

7.1 Authentication request scenarios

Three general classes of authentication request exist:

- user initiates authentication request;
- NO initiates authentication request;
- SP initiates authentication request.

Authentication request scenarios may involve all authentication framework procedures.

7.1.1 Scenario S1: User initiates authentication request

7.1.1.1 Scenario S1A: New registrations, no roaming agreement exists

Pre-requisites:

- user is not registered with NO
- NO and user's SP do not have a roaming agreement

Initiating action:

- user initiates authentication request (as part of a registration attempt)

Authentication framework procedures involved:

- P1, P2, P3, P4, P5

Message flow diagram:

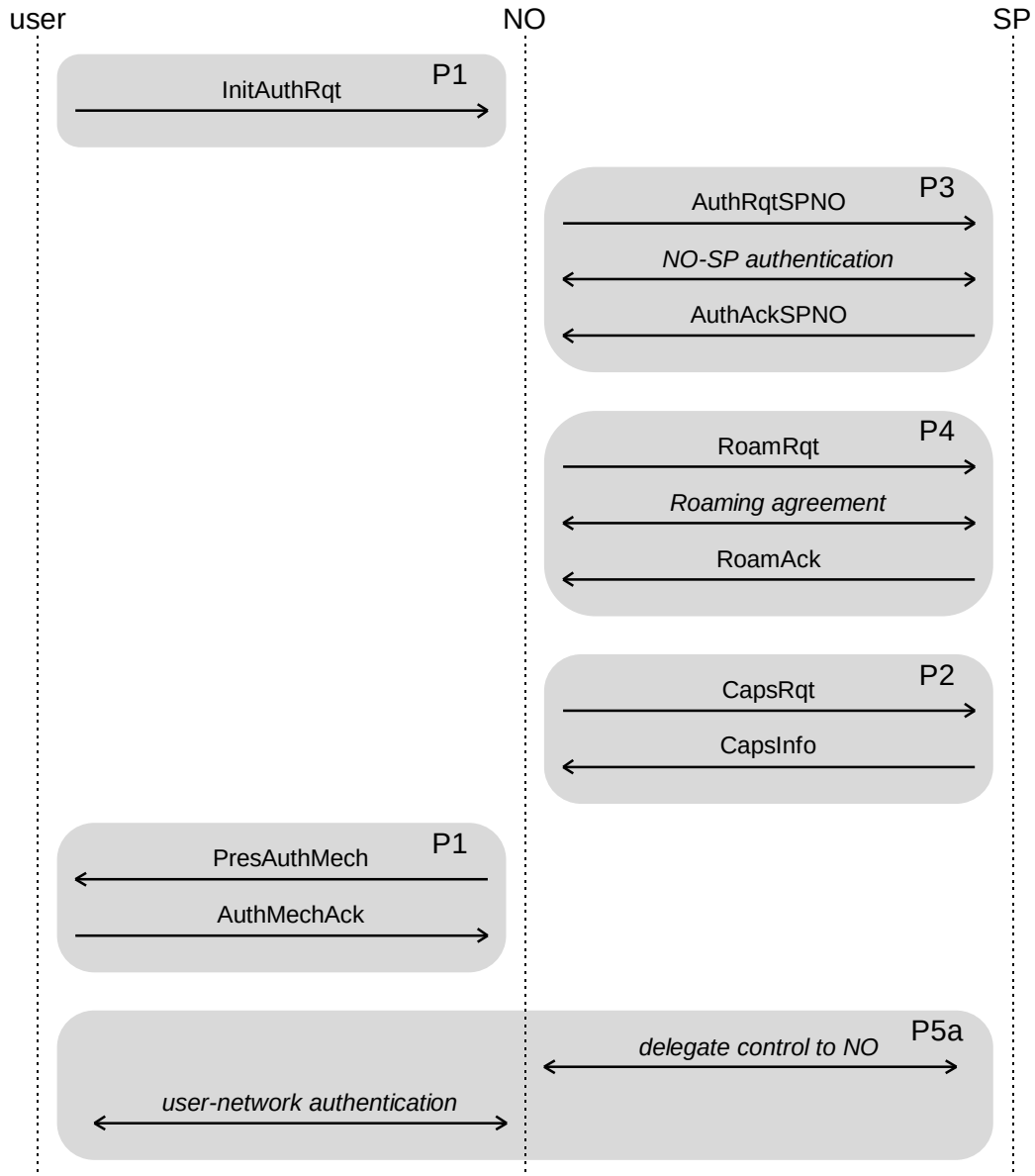


Figure 7-1 Message flow diagram for scenario S1A

Description:
The user sends an initial message to a NO - this will include the user's service provider, authentication capability class, but not his identity nor his temporary identity. The NO does not have a roaming agreement with the SP so it initiates a procedure to establish one dynamically - if one cannot be established dynamically, then the request is refused. A procedure to establish a roaming agreement begins with the NO and SP authenticating each other. After authentication the NO and SP negotiate a roaming agreement which will involve each party digitally signing the agreement. Once an agreement has been established, the NO sends the user's authentication capability class to his SP. The SP will respond by providing the NO with the authentication capabilities of that particular authentication capability class - this will include the authentication mechanisms the user is capable of handling. The NO will then choose an authentication mechanism based on information about the authentication capabilities of itself, the SP and the user. The NO then sends the identity of the prescribed mechanism to the user. The authentication mechanism for new registrations involving the SP, NO and user is initiated. Note, however, that the SP may choose to delegate the actual authentication to a Certification Authority (CA).

7.1.1.2 Scenario S1B: New registrations, roaming agreement exists

Pre-requisites:
- user is not registered with NO
- NO and user's SP do have a roaming agreement

Initiating action:
- user initiates authentication request (as part of a registration attempt)

Authentication framework procedures involved:
- P1, P2, P5

Message flow diagram:

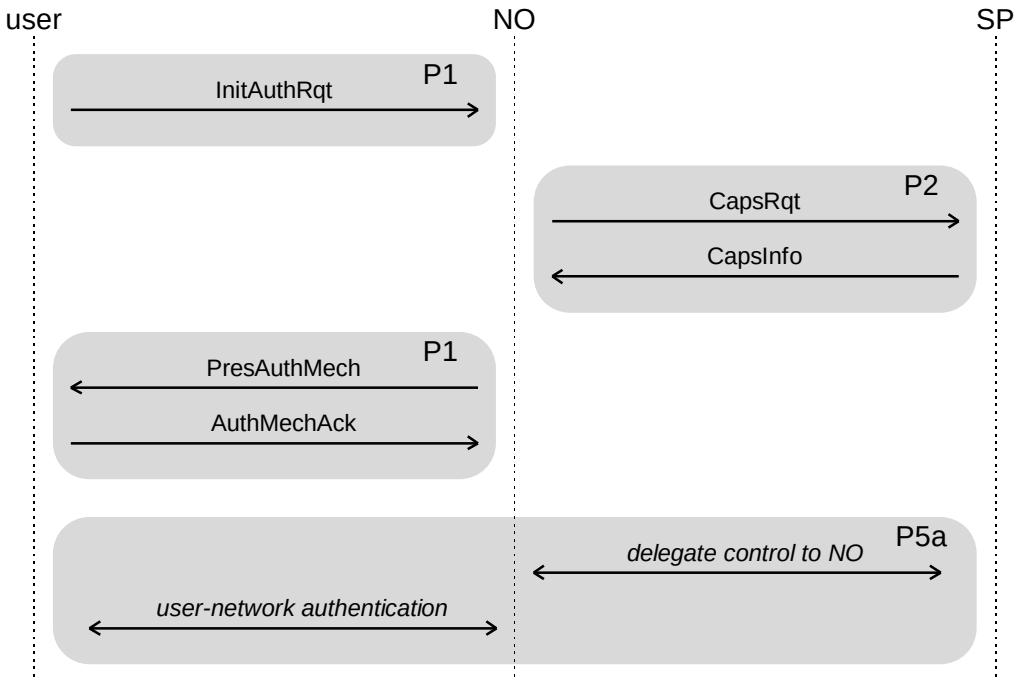


Figure 7-2 Message flow diagram for scenario S1B

Description:
A user sends an initial message to a NO - this will include the user's service provider, authentication capability class, but not his identity (or temporary identity). The NO recognises that it has a roaming agreement with the SP. A check is made by the NO to see if the roaming agreement has been revoked, if so then either the request may be refused, or an attempt may be made to establish a new roaming agreement. Once the agreement has been verified, the NO sends the user's authentication capability class to his SP. The SP will respond by providing the NO with the specification of that particular authentication capability class - this will include the authentication mechanisms the user is capable of handling. The NO will then choose an authentication mechanism based on information about the authentication capabilities of itself, the SP and the user. The NO sends the identity of the prescribed mechanism to the user. The authentication mechanism for new registrations involving the SP, NO and user is then initiated. Note, however, that the SP may choose to delegate the actual authentication to a Certification Authority (CA).

7.1.1.3 Scenario S1C: Current registrations

Pre-requisites:
- user is registered with NO

Initiating action:
- user initiates authentication request (may be as part of a service request)

Authentication framework procedures involved:
- P1, P5

Message flow diagram:

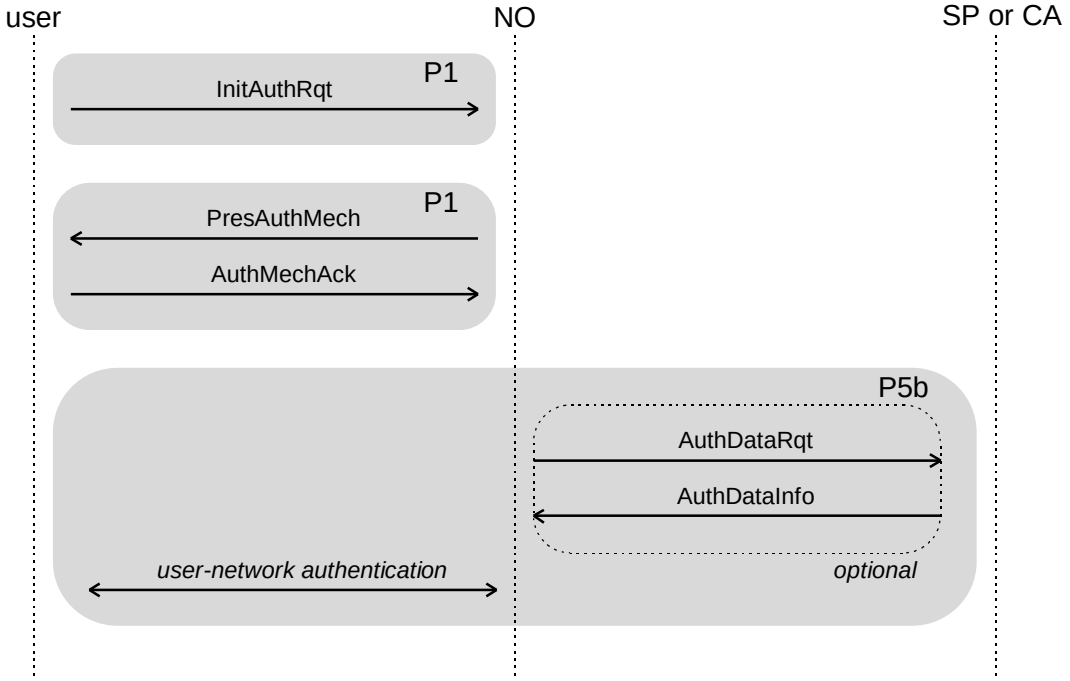


Figure 7-3 Message flow diagram for scenario S1C

Description:
User sends an initial message to a NO - this will include the user's service provider, authentication capability class, but not his identity (or temporary identity). The NO recognises that it has a roaming agreement with the SP. A check is made by the NO to see if the roaming agreement has been revoked, if so then the request is refused. Once an agreement has been verified the NO will look up the user details which have been previously registered. The NO will then choose an authentication mechanism, based on information about the authentication capabilities of itself and the user. The NO sends the identity of the prescribed mechanism to the user. The authentication mechanism for current registrations involving the NO and user is initiated. This mechanism includes an option for the NO to request authentication data from the user's SP if required. Note, however, that the SP may choose to delegate the actual authentication to a Certification Authority (CA).

7.1.2 Scenario S2: NO initiates authentication request

Pre-requisites:

- user is registered with NO

Initiating action:

- NO initiates authentication request

Authentication framework procedures involved:

- P1, P5

Message flow diagram:

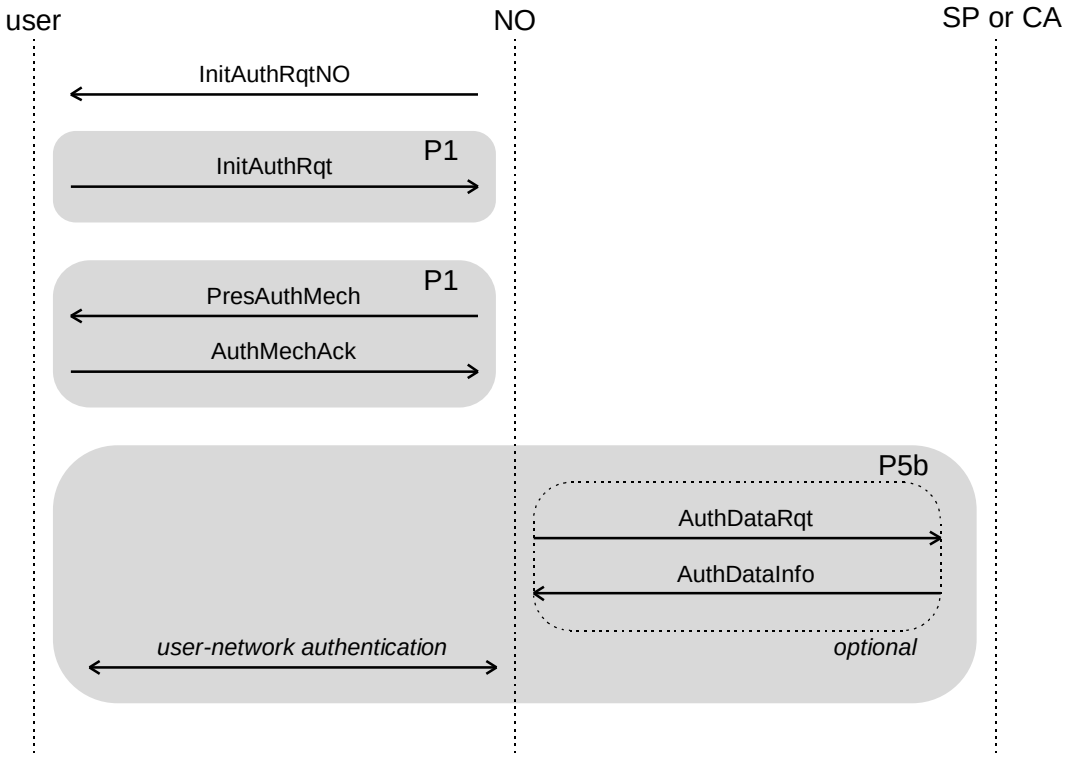


Figure 7-4 Message flow diagram for scenario S2

Description:

NO sends an initial message to the user instructing him to make an authentication request. The user then sends an initial authentication request message to a NO - this will include the user's service provider, authentication capability class, but not his identity (or temporary identity). The NO recognises that it has a roaming agreement with the SP. A check is made by the NO to see if the roaming agreement has been revoked, if so then the request is refused. Once an agreement has been verified the NO will look up the user details which have been previously registered. The NO will then choose an authentication mechanism, based on information about the authentication capabilities of itself and the user. The NO sends the identity of the prescribed mechanism to the user. The authentication mechanism for current registrations involving the NO and user is initiated. This mechanism includes an option for the NO to request authentication data from the user's SP if required. Note, however, that the SP may choose to delegate the actual authentication to a Certification Authority (CA).

7.1.3 Scenario S3: SP initiates authentication request

Pre-requisites:

- user is registered with NO

Initiating action:

- SP initiates authentication request

Authentication framework procedures involved:

- P1, P5

Message flow diagram:

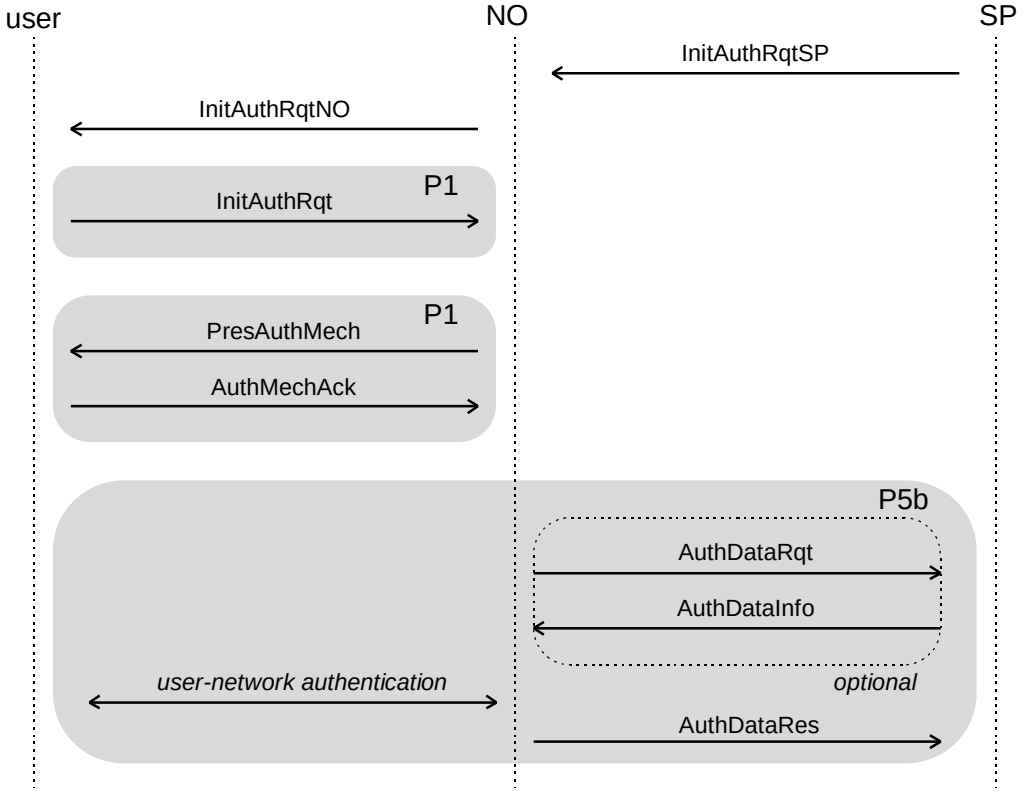


Figure 7-5 Message flow diagram for scenario S3

Description:

SP send an initial message to the NO. The NO responds to this message by sending an initial message to the user instructing him to make an authentication request. The user then sends an initial authentication request message to a NO - this will include the user's service provider, authentication capability class , but not his identity (or temporary identity). The NO recognises that it has a roaming agreement with the SP. A check is made by the NO to see if the roaming agreement has been revoked, if so then the request is refused. Once an agreement has been verified the NO will look up the user details which have been previously registered. The NO will then choose an authentication mechanism, based on information about the authentication capabilities of itself and the user. The NO sends the identity of the prescribed mechanism to the user. The authentication mechanism for current registrations involving the NO and user is initiated. This mechanism includes an option for the NO to request authentication data from the user's SP if required. Subsequent to the user-network authentication, the NO informs the SP of the result of the authentication exchange.

7.2 Roaming agreement request scenarios

Two general classes of roaming agreement request exist:

- NO initiates roaming agreement request;
- SP initiates roaming agreement request.

Roaming Agreement request scenarios involve only authentication framework procedures P3 and P4.

7.2.1 Scenario S4: NO initiates roaming agreement request

7.2.1.1 Scenario S4A: SP and NO have not authenticated

Pre-requisites:

- NO and SP have not authenticated

Initiating action:

- NO initiates roaming agreement request

Authentication framework procedures involved:

- P3, P4

Message flow diagram:

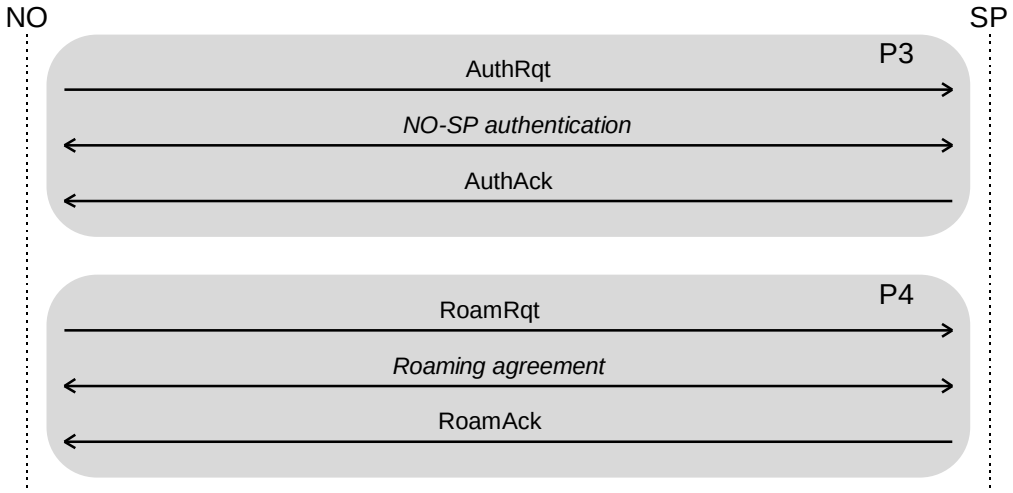


Figure 7-6 Message flow diagram for scenario S4A

Description:

If a NO does not have a roaming agreement with a SP he can initiate a procedure to establish one at any time - this may or may not be done dynamically (that is, it may or may not be done automatically by means of the procedure P4). The procedure to establish a roaming agreement begins with the NO and SP authenticating each other. The agreement is established once the NO and SP have (digitally) signed it.

7.2.1.2 Scenario S4B: SP and NO have authenticated

Pre-requisites:

- NO and SP have authenticated

Initiating action:

- NO initiates roaming agreement request

Authentication framework procedures involved:

- P4

Message flow diagram:

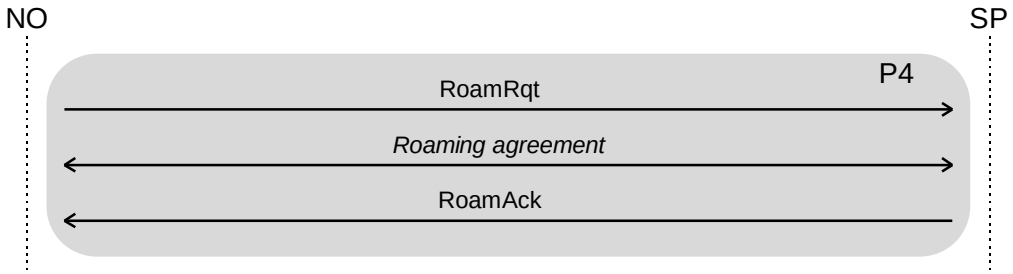


Figure 7-7 Message flow diagram for scenario S4B

Description:
If a NO does not have a roaming agreement with a SP he can initiate a procedure to establish one at any time - this may or may not be done dynamically. The agreement is established once the NO and SP have (digitally) signed it.

7.2.2 Scenario S5: SP initiates roaming agreement

7.2.2.1 Scenario S5A: SP and NO have not authenticated

Pre-requisites:
- NO and SP have not authenticated

Initiating action:
- SP initiates roaming agreement request

Authentication framework procedures involved:
- P3, P4

Message flow diagram:

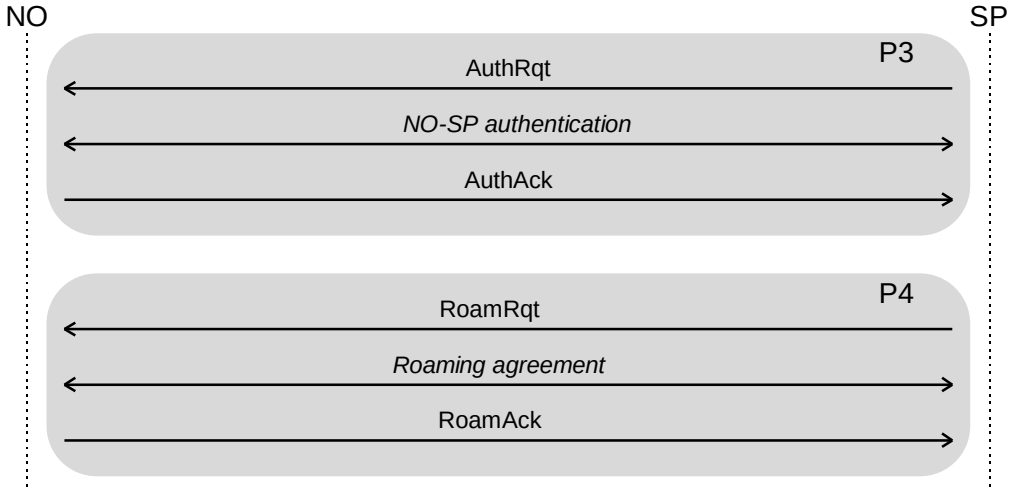


Figure 7-8 Message flow diagram for scenario S5A

Description:
If a SP does not have a roaming agreement with a NO he can initiate a procedure to establish one at any time - this may or may not be dynamic. The procedure to establish a roaming agreement begins with the NO and SP authenticating each other. The agreement is established once the NO and SP have (digitally) signed it.

7.2.2.2 Scenario S5B: SP and NO have authenticated

Pre-requisites:
- NO and SP have authenticated

Initiating action:
- SP initiates roaming agreement request

Authentication framework procedures involved:
- P4

Message flow diagram:

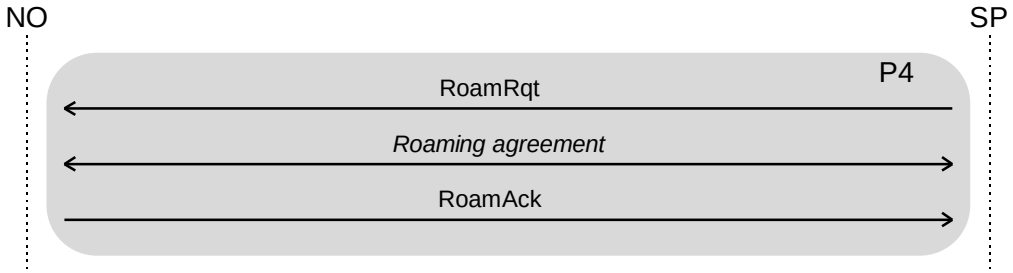


Figure 7-9 Message flow diagram for scenario S5B

Description:
If a SP does not have a roaming agreement with a NO he can initiate a procedure to establish one at any time - this may or may not be done dynamically. The agreement is established once the NO and SP have (digitally) signed it.

7.3 Scenarios involving GSM subscribers

In order to demonstrate migration to UMTS another scenario, initiated by a GSM user, is possible. The GSM user should be able to roam onto the UMTS network, be adequately authenticated and receive appropriate security services. This case should proceed as in the above scenarios. However, once the user is recognised as a GSM user, the mechanism employed for user-network authentication will be the GSM authentication mechanism. This scenario is for further study.

8. Description of the Intermediate "Evolutionary Levels"

According to the generic framework presented in section 3, security migration aspects are investigated at each "transition phase". In particular, the actions that should take place at each "transition phase" are:

- Investigation of additional security features that could be supported by the next "evolutionary level".
- Selection of the "appropriate" security mechanisms. The selection will be based on: (a) the available ("proposed") mechanisms and *(b) some evaluation study (performance, feasibility, etc.).*
- Identification of new interfaces and protocols relevant to security.
  (in conjunction with the previous "level" status)
- Derivation of the information flows which comprises, the identification of exchanged messages[16], the message structure and the information elements conveyed.
- Identification of new requirements (security algorithms, functionality, interfaces, protocols) concerning terminals, SIMs, access and core network.

The material included in this section, is organised as follows. Subsection 8.1 presents some general considerations regarding the intermediate "evolutionary levels" (ASPeCT level 2 and 3). Subsection 8.2 includes some ideas on the selection of the security features to be provided by the intermediate levels. Subsection 8.3 presents a proposal to introduce security enhancements in the different intermediate levels of the migration path.

8.1 General Considerations

The intermediate "evolutionary levels", considers a GSM/DECT operator that has enhanced its functionality (introduction of the UMTS-SCP) to enable roaming of UMTS users between GSM/DCS and DECT systems (" ASPeCT level 2 and level 3). UMTS users can be conceived as the:

- new users equipped with a multi-application UMTS UIM. These users which will have access to "advanced" UMTS-like services and features offered by the GSM/DCS/DECT network infrastructure using appropriate terminal types[17]. The same UIM could be possibly used (in the future) for accessing UMTS services via UMTS terminals provided that care has already been taken regarding authentication algorithms, service profiles, etc.
- GSM/DCS/DECT users who wish to enhance their set of services by adding new UMTS-like services and features. These users will have to change their SIM/DAM (to a multi-application UIM).

Note: UMTS terminals are not considered for ASPeCT level 2, due to the absence of the UMTS radio interface. However, due to the different evolution/migration path could be followed by the network operators (see section 3), multi-mode terminals supporting UMTS access may be available in the market. UMTS access will be permitted as soon as UMTS BSSs will operate in a new frequency band (ASPeCT level 3).

8.2 Selection of the Security Features

Obviously, the security features envisaged for the intermediate "evolutionary levels" will be a compromise of the security features expected to be offered by third generation mobile systems. Based on this fact, two approaches can be foreseen:

- The evolution (improvement or upgrade) of the contemporary GSM/DECT security features by implementing new, advanced security mechanisms.
- The support of a subset of the security features expected to be offered by the UMTS. Table 1 presents an indicative, comparative list of the security features offered by the second generation mobile systems (GSM, DECT) and the expected for third generation systems [2].

Among the issues that have to be dealt with during the application of the aforementioned approaches (or a combination of these) are:

- The derivation of the criteria for the selection of UMTS security features. A non-exhaustive list of such criteria can be found in [1]. Among them, the fitness for purpose, the security proof, the number of

[16] Some investigation is needed to check whether previous "level" protocols can support new messages. If required, new protocols should be defined.

[17] A limited set of UMTS services will be offered at this level, due to the absence of the UMTS air interface. The maximum bitrate will be restricted by the corresponding limitations of the GSM and DECT radio interfaces.

messages, the length of messages, the performance effects, the key storage, the need for security servers are included.

- The selection of the corresponding security mechanisms to be supported by the intermediate "evolutionary levels". At this stage, possible inter-relations between security features and mechanisms should be investigated , since security features often depend on other security features or functions for their operation. For example, user data confidentiality requires encryption.
- The impact of the selected features on the existing security protocols. The support of the new features over the existing protocols needs investigation.
- The conformance to the relevant GSM/DECT standards.

It is apparent that the selection of the "appropriate" security features/mechanisms for the intermediate "evolutionary levels" is a very difficult task due to the various parameters introduced.

Security Features	GSM	DECT	UMTS
Confidentiality/Anonymity			
User Traffic Confidentiality: This element protects against unauthorised eavesdrropping on user traffic	**Y**	**Y**	**Y**
User Identity Confidentiality: an element by which the identity of a user is protected against disclosure over a radio interface	**Y**	**Y**	**Y**
User Location Confidentiality: an element by which the physical location of a user is protected against disclosure over a radio interface			**Y**
Signalling Data Confidentiality: this element ensures that the signalling data is not made available or disclosed to unauthorised parties	**Y**	**Y**	**Y**
Confidentiality of Stored Data: This element ensures that stored data is not made available or disclosed to unauthorised parties			**Y (T)**
Integrity			
User Traffic Integrity: This element protects against manipulation (modification, insertion and/or replay) by unauthorised parties of user data on the radio path			**Y**
User Location Integrity: an element by which the service provider and/or network operator can have some assurance that the user location related information cannot be modified by the intruders (Note 1)			
Terminal Location Integrity: an element by which the service provider and/or the network operator can have some assurance that the mobile terminal location related information cannot be modified by the intruders. (Note 1)			
Integrity of Stored Data: This element offers protection for stored data against unauthorised writing and modifying.			**Y(T)**
Signalling Data Integrity: This element provides protection against manipulation (modification, insertion or replay) by unauthorised parties of signalling data			**Y**
Authentication			
Authentication of SP to User: This element provides corroboration of the identity of a service provider to a user			**Y**
Authentication of User to SP: This element provides corroboration of the claimed identity of a user to a service provider			**Y**
User Identity Authentication : An element by which the identity of a user is verified to be the one claimed	**Y(2)**	**Y(3)**	**Y(2)**
Authentication of Terminal to Terminal Manager: This element provides corroboration of the identity of a terminal to a terminal manager	**Y(4)**		**Y(S)**
Authentication of Providers: This element provides corroboration of the identity of one network operator or service provider to another			**Y(S)**
Authentication of NO to User (Terminal): This element provides corroboration of the identity of a network operator to a user		**Y(5)**	**Y**
Authentication of User (Terminal) to NO: This element provides corroboration of the claimed identity of a user to a network operator	**Y**	**Y(5)**	**Y**
Re-authentication of Users: An element by which the identity of a user is re-verified to be the one claimed. This feature may be invoked repeatedly or at any appropriate instant.	**Y**	**Y**	**Y**
Re-authentication of Terminals: An element by which the identity of a terminal is re-verified to be the one claimed. This feature may be invoked repeatedly or at any appropriate instant.			**Y**
Non-Repudiation			
Non-repudiation of Origin of Signalling and Control Data: This element provides proof to a third party that a message was sent by a certain entity.			**Y(6)**

Non-repudiation of Delivery of Signalling and Control Data: This element provides proof to a third party that a message was received by a certain entity.			**Y(6)**
Non-repudiation of Access to Stored Data: This element provides protection against an entity denying having attempted to access stored data.			**Y(T)**
Access Control			
Access Control to SIM/DAM/UIM: This element ensures that a SIM/DAM/UIM can only be used by an authorised party.	**Y**	**(7)**	**Y**
Access Control to Terminal Equipment: This element ensures that terminal equipment can only be utilised by authorised parties.			**Y**
Access Control to Service Profile: This element ensures that only authorised parties can access a service profile			**Y**
Access Control to Subscription Data: an element by which there are restrictions in the access to the personal data of a user or subscriber stored in the network.		**Y(8)**	
Access Control to Telecommunication Services: This element ensures that only authorised parties can access a telecommunication service			**Y**
Management of Security			
Negotiation of authentication mechanisms: allowing a flexible way to support different mechanisms and algorithms to be incorporated, with the ability to migrate smoothly from one mechanism to another			**Y**
Dynamically set-up of Roaming agreement: in order to facilitate roaming, roaming agreements can be set-up as and when they are required.			**Y**
Supplementary			
Support of end-to-end Security Services			**Y**

Table 8-1: Comparison of Second and 'expected' Third Generation Security Features

(T) means that the definition of the associated mechanism has been assigned tertiary priority within ETR 050901.

(S) means that the definition of the associated mechanism has been assigned secondary priority within ETR 050901.

Note 1: if user location and terminal location are seen as being part of the signalling data, then integrity of the last implicitly implies the user/terminal location integrity.

Note 2: user identity authentication towards the SIM / UIM

Note 3: user identity authentication towards the home network

Note 4: In GSM the terminal identity is checked towards a list of blacklisted identities.

Note 5: In DECT the user and terminal authentication are identical, the user is uniquely linked to a terminal. This is only so when the DAM is not used. When the DAM is used by the user, terminal authentication is no longer provided.

Note 6: This is only provided to enable prove of access to telecommunication services and access/change to service profiles.

Note 7: only applicable if the DAM is used and then it is provided.

Note 8: this is included in the access control to stored data within the service providers and network operators.

8.3 Security enhancements in the different levels

8.3.1 ASPeCT Level 2

A. SIM/UIM

New users are provided with multi-application (pre-)UMTS UIMs. These UIMs are backward compatible with the GSM/DECT smart card commands defined for GSM SIM and DECT DAM. However, a problem may occur at the introduction time if the appropriate standards for UMTS are not ready at the period. The UMTS UIM should be at least compliant with all the ISO standards (7816-series : support all approved/standardised commands). It will support both authentication GSM/DECT algorithms and possibly newly supported UMTS security features.

The UMTS user is provided with UMTS identifiers. GSM/DECT identifiers can be deducted from these UMTS identifiers, supporting full compatibility with the GSM/DECT network.
The UMTS user is known to the GSM/DECT network by its UMTS identifiers stored either in the UMTS/GSM SCP or in the GSM/UMTS HLR/AC/EIR. The GSM Ph2+ MSC/VLR can interface with the UMTS enhanced SCP or the HLR/AC/EIR.
The GSM/DECT security features will still be provided: user identity confidentiality, user authentication to the network, Kc for encryption over the air interface. The GSM/DECT authentication algorithm will use as input parameters uniquely derived from UMTS parameters.

B. Terminal Equipment
The terminal equipment functionality does not need any upgrade compared to the ASPeCT level 1 ("initial network situation"). The previous phase terminals are still operational.

C. Access and Core Network Functionality
The new A-interface will be introduced between the BSS and the UMTS/GSM MSC/VLR. The mobility management procedures will be changed
The UMTS/GSM SCP and/or the GSM/UMTS HLR/AC/EIR should be upgraded compared to the previous level functionality so as to store and manage UMTS and GSM identifiers.

D. New Security Interfaces and Protocols
Compared to the ASPeCT level 1, the UMTS/GSM SCP - UMTS/GSM HLR/AC/EIR interface is introduced and should be specified. The relevant protocol should be specified.
No new security features are introduced.

In the following paragraph a possible mapping between the GSM parameters relevant for security and the UMTS parameters (as they are known at the moment) is made. The UMTS parameters are mapped upon GSM parameters, which will be used in the GSM network to identify the user and to offer the GSM security features :

- IMSI
  UMTS uses an International Mobile User Identity (IMUI).
  In order to allow registration of a UMTS subscriber in a GSM network, his IMUI must contain at least the same fields as the IMSI namely :
  - Mobile Country Code, maximum 3 digits
  - Mobile Network Code, maximum 2 digits
  - A number by which the home service provider can identify the subscriber, maximum length 10 digits

  The IMUI can be longer, even particular parts, as long as at this point in time only limited digits are used, there is no problem.
- TMSI
  UMTS may use temporary identities generated by the visited network, as in GSM. In UMTS they are called TMUI.
  The TMSI has only significance in the area controlled by the VLR that allocated the number. There is no need to map TMSI's to TMUI's.
- RAND
  In all three proposed authentication mechanisms ([6]) the network operator generates a random value RND_N. In order to allow mapping to the GSM random RAND, the length of RND_N must be at least 16 bytes. (The first byte of RAND is the Information Element Identifier).
- SRES
  No mapping is necessary, because the GSM security mechanisms are used, so SRES is calculated from Ki and RAND.
- Ki
  No mapping from GSM to UMTS. It would only be relevant for secret key based mechanisms in UMTS where it is better to define UMTS specific keys.
- Kc
  No mapping is necessary, because the GSM security mechanisms are used, so Kc is calculated from Ki and RAND.

- IMEI
  It must be possible to derive the structure of the IMEI uniquely from the IMTI, which is the UMTS equivalent of the GSM IMEI
- Ciphering Key Sequence Number
  No equivalent is foreseen in UMTS.

8.3.2 ASPeCT Level 3

A. SIM/UIM
Depending on the security capabilities of the previous UMTS UIM version (full or partial support of the UMTS security features), a new UIM may be required.

B. Terminal Equipment
At this level, adaptive, multi-mode UMTS terminals operating in both GSM/DCS/DECT and UMTS radio interfaces will be introduced. These terminals should support the new security interface between the terminal and the UMTS BSS. The other terminal types (GSM/DCS/DECT) are not affected.

C. Access and Core Network Functionality
The access system is enhanced by the introduction of the UMTS air interface. The new A-interface will be introduced between the BSS and the UMTS/GSM MSC/VLR. The mobility management procedures will be changed, as an evolvement of the GSM phase 2+ procedures.
The core network will not support all UMTS features yet, enhancements will be necessary to support the new A-interface, the changed mobility management procedures and for the handling of the increased (signalling and traffic) load, expected by the increase of the UMTS user penetration rate.

D. New Security Interfaces and Protocols
Due to the fact that changes are foreseen in the A-interface and the mobility management procedures, to which the security procedures are closely linked, almost all UMTS security features could be introduced. The introduction of UMTS in steps, according to the different levels, a need is caused to priorise the introduction of the UMTS security features and their associated mechanisms. A proposal is made hereafter.
The introduction of security features, will also have impact on the GSM/UMTS MSC/VLR - GSM/UMTS SCP interface.

security procedures / features	Y/N	motivation
Authentication Framework		
Procedure P1: User-No authentication capability agreement	Y	This is the negotiation of the authentication mechanism/capabilities between the user and the network operator: early introduction eases compatibility. This procedure is also closely linked to the mobility management procedures.
Procedure P2: NO-SP authentication capability agreement	N	although this is an essential part of the negotiation phase, the proposal is to delay this because it implies an interface change between the NO and the SP
Procedure P3: Service provider- network operator authentication	N	This is a change between the NO and the SP interface and is not necessary when P2 and P4 are not introduced
Procedure P4: Establishment of NO-SP roaming agreement	N	In this level, existing off-line roaming agreements will be used
Procedure P5: User-network authentication	Y	This replaces the authentication in the GSM/DECT network. Mutual authentication from the NO to the User is provided. Depending on the mechanism also authentication from the SP to the User is provided. Introducing UMTS authentication implies also that the user identity confidentiality and key

		agreement are offered. Some mechanisms also supply support for non-repudiation. An interface change towards the home network is needed, to pass the necessary security parameters.
Confidentiality / Anonymity		
confidentiality of the air interface	Y	The key agreed in the authentication procedure can be used on the air interface to encrypt..
User identity anonymity	Y	This has to be guaranteed, by a good definition and interaction between the MM procedures and the security procedures
Integrity		
Integrity of sent data	N	
Access control		
Access control to equipment	Y	
Access control to a service	Y/N	partly provided by existing mechanisms
Access control to data	N	
Non - repudiation		
Non-repudiation of origin of transmitted data	Y/N	partly when possible within authentication mechanism
Non-repudiation of delivery of transmitted data	Y/N	partly when possible within authentication mechanism
Non-repudiation of access to data	N	
Non-repudiation of access to services	N	
Non-repudiation of procedure involvement	N	
Authentication		
Entity authentication	Y	see P5 of the authentication framework
Transmitted data origin authentication	N	

9. Functional description of the demonstrator

This section describes what will be demonstrated in the first demonstrator on a high level : which migration scenario, which authentication protocol will be used, the interface to the user ...

9.1 Goals of the demonstration

The aim of the demonstration is to show the validity of the UMTS migration protocol and the feasibility of implementing a migratory UIM.

In the first demonstration a simplified version of the migration scenarios will be implemented. The feasibility of adding the authentication framework together with UMTS authentication protocols will be showed. The migratory UIM will be described in D06.

9.2 Features

9.2.1 Logical structure of the demo configuration

The following logical entities (roles) can be involved in the security protocols (See Figure 9-1):

- The User: he is authorised by a subscriber to make use of the telecommunication services, the subscriber subscribed to by the service provider.
- The network operator: provides the network capabilities necessary for the support of the services or set of services offered to the users.
- Service Provider : has overall responsibility for the provision of a service or set of services to users associated with a subscription and for negotiating the network capabilities associated with that service or set of services with network operators.

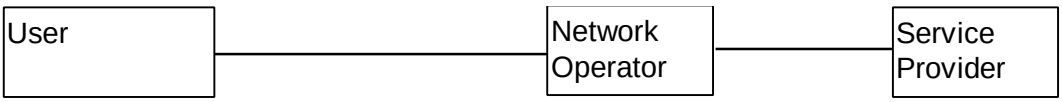


Figure 9-1 : WP2.1 demonstration logical structure

9.2.2 Description of the demonstrated features

9.2.2.1 New registrations, roaming agreement exists

The user is not registered with the NO, the NO and user's SP do have a roaming agreement. The NO has no security related data for the user.

The user initiates the authentication.

The protocol executed here corresponds with Scenario S1B from the authentication framework (see chapter 5 and 7), for the user-network authentication two options will be implemented:

- the challenge response mechanism using symmetric key techniques - New Registration (see section 7.3.2.2.2 in [6])
- A public key based mechanism - Protocol B (see section 7.3.2.3.2 in [6])

The prerequisites apply as described in [6].

The user wants to register and sends a registration request to the network. The network recognizes that it has a roaming agreement for the user's service provider. The NO will receive the authentication capabilities from the registered user by the SP. An authentication mechanism will be negotiated between the NO and the user.

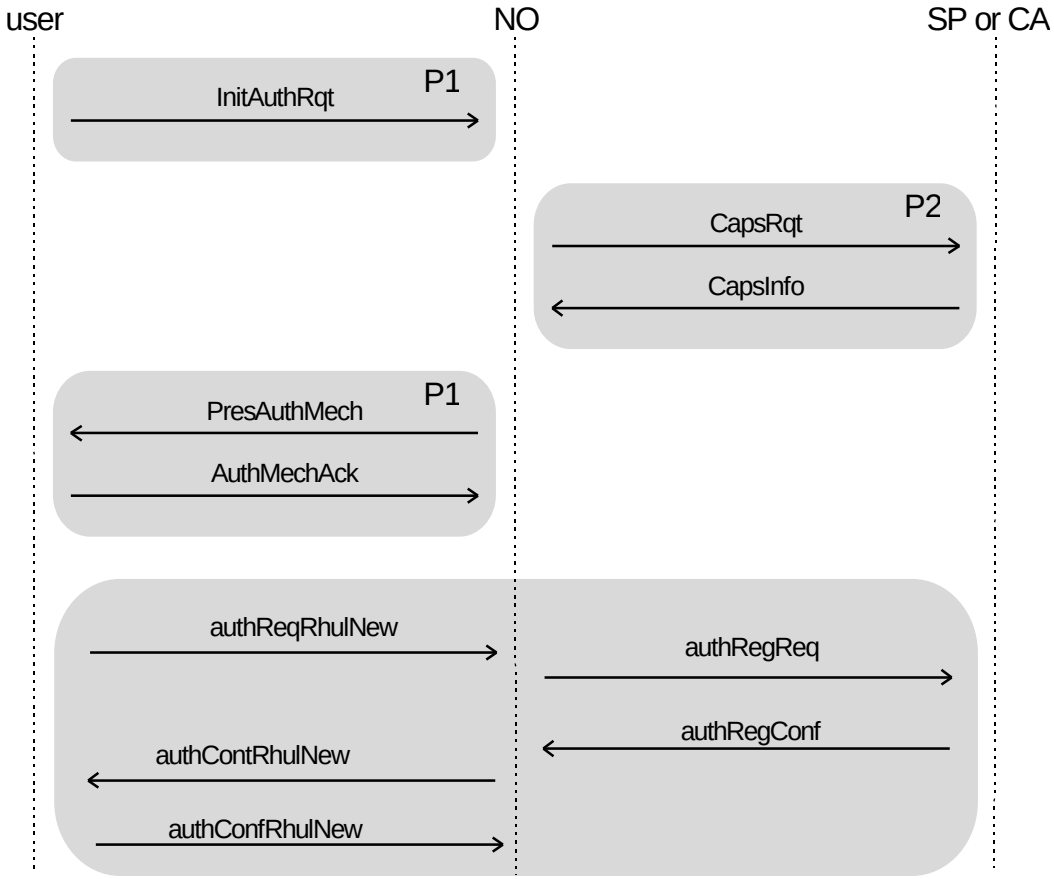


Figure 9-2 : New Registration : Symmetric key authentication

The symmetric key authentication has been chosen. This mechanism requires that authentication parameters have to be requested from either the user's SP or a CA approved by the SP.

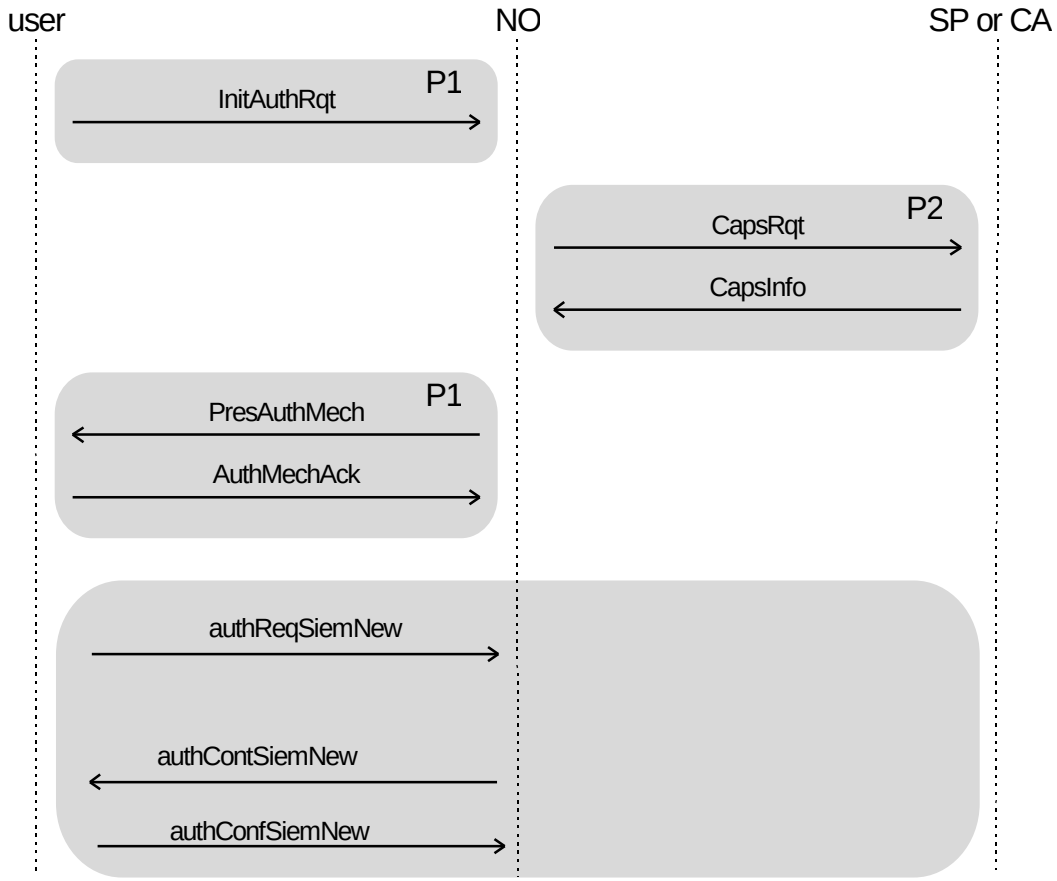


Figure 9-3 : New Registration : Public key authentication

The public key based authentication mechanism has been chosen, no authentication parameters have to be retrieved from the SP. The mechanism is based on the use of certificates, the NO and the user have to have a common certification authority. The communication with the certification authority is not shown on these flows, that can be done completely off-line. This means that public certificates may be retrieved by the NO from the CA (for the respective authentication capability classes), in advance of any user undergoing authentication.

9.2.2.2 NO initiates authentication request

The user is registered with the NO, the NO has security related data for the user. The NO initiates the authentication.

The protocol executed here corresponds with Scenario S2 from the authentication framework (see chapter 5 and 7), for the user-network authentication two options will be implemented:

- the challenge response mechanism using symmetric key techniques - Current Registration (see section 7.3.2.2.1 in [6])
- A public key based mechanism - Protocol A (see section 7.3.2.3.1 in [6])

The prerequisites apply as described in [6].

The NO wants to authenticate a registrated user and sends the appropriate message to the user. The No has all necessary data of the user, it has a roaming agreement with the SP and knows the users authentication capabilities. An authentication mechanism will be negotiated between the NO and the user.

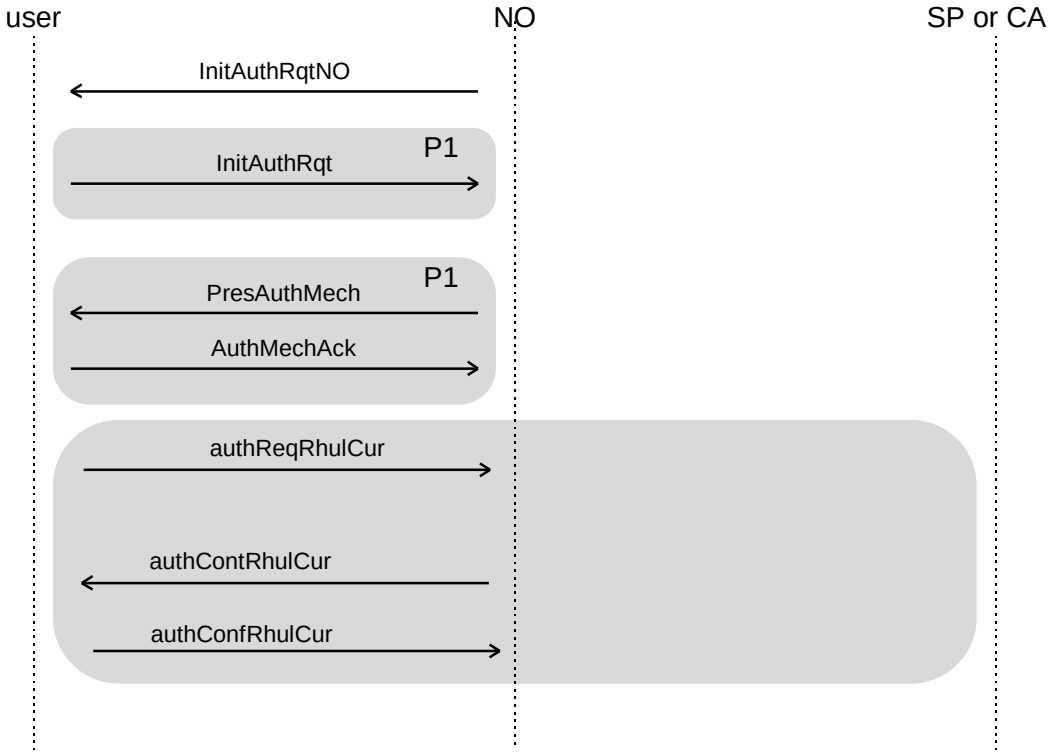


Figure 9-4 : Current Registration : Symmetric key authentication

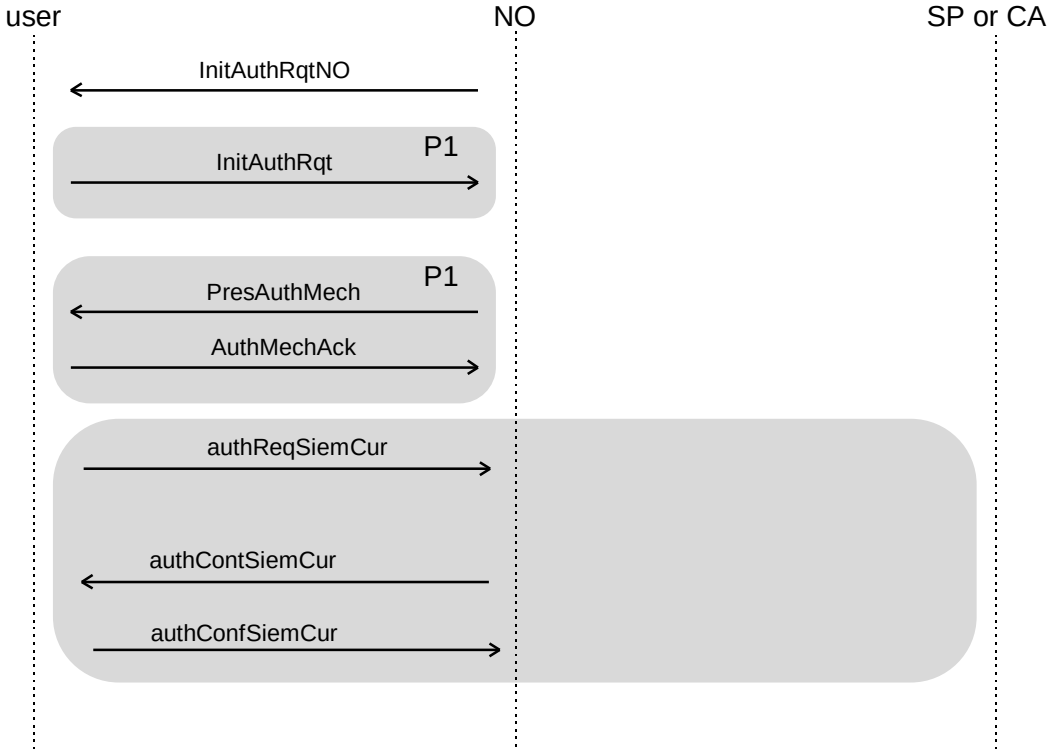


Figure 9-5 : Current Registration : Public key authentication

9.2.3 Interaction with the demonstrator users

In each role actions can be initiated by the user of the demonstrator. A graphical user interface will be provide enabling following commands for the different roles:

9.2.3.1 GUI requirements for the user

The user can initialise, change and display its profile, this includes identification parameters as well as the security parameters, the authentication capabilities and mechanisms he supports.

The user can register to the network. At registration the New registration protocol will be started with the parameters as provided in the users profile.

The user's status (registered yes or no) can be displayed and reset from registered to not registered.

The user will see that a protocol is running and can stop the protocol at any time. This simulates getting towards an uncovered area, ...

Errors and/or inconsistencies during protocol execution will be displayed on the screen.

9.2.3.2 GUI requirements for the network operator

The network operator can change and display its profile, this includes identification parameters, authentication capabilities, roaming agreements, security parameters, e.g. certificates

The network operator can initiate an authentication to a registrated user. The Current registration protocol will be started with the parameters as provided in the network operators profile.

The list of registered users can be displayed. The user's status (registered yes or no) can be reset from registered to not registered.

The network operator will see that a protocol is running and can stop the protocol at any time, this simulates all kinds of network, congestion problems, ...

Errors and/or inconsistencies during protocol execution will be displayed on the screen.

9.2.3.3 GUI requirements for the service provider

The service provider can change and display its profile, this includes identification parameters, authentication capabilities, roaming agreements.

Users can be created, changed, deleted, displayed at the service provider. The user's profile can be created or modified.

The service provider will see that a protocol is running and can stop the protocol at any time, this simulates all kinds of network, congestion problems, ...

Errors and/or inconsistencies during protocol execution will be displayed on the screen.

9.3 Defining System architecture

9.3.1 Physical structure of the demonstration

The following demonstration structure is required :

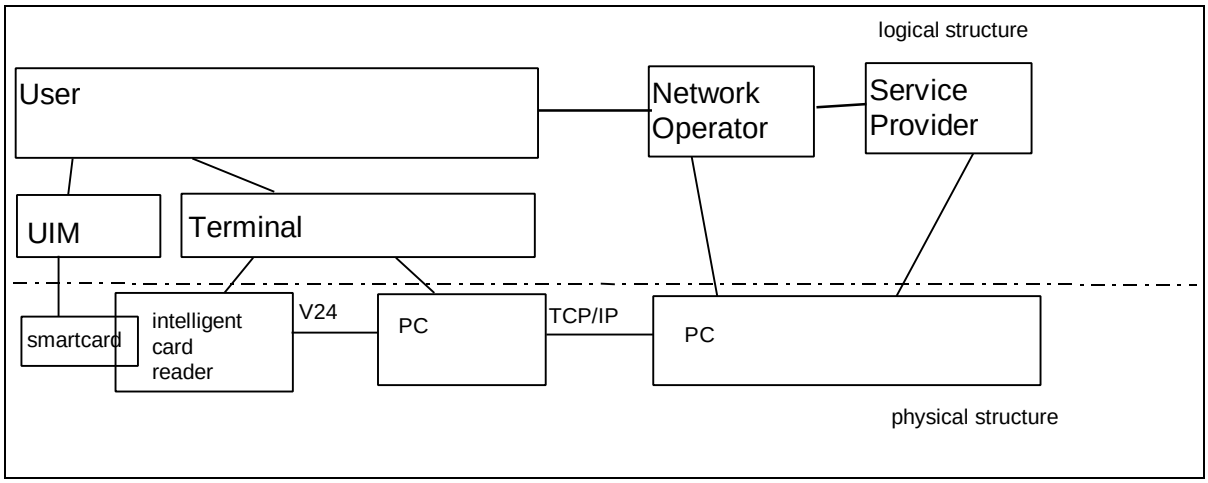


Figure 9-6 : WP2.1 demonstration mapping of physical structure to logical structure

The user is represented by the UIM. The user's profile and authentication data and procedures are all available on the smartcard. The UIM contains the service providers knowledge of the user and is delivered by the service provider. For more information on the smartcard, see D6.

The user accesses the network via a terminal. The UMTS terminal functionality has been split up into two parts:

- The intelligent card reader: interfacing directly with the smartcard, which features a display and keyboard, similar to a conventional mobile phone
- A PC: mainly containing the GUI for the user and the protocol handling towards the network as well as towards the ICR.

The ICR and the PC are connected via a V24 interface.

The Network operator and the service provider are both realized on a PC. One PC contains both the entities. The designed GUI will allow an easy distinction between the NO and the SP. The NO and the SP will communicate via internal message queues.

In a real life situation the Network operator communicates with the mobile terminal via the air interface and base stations. For this demonstration, no air interface is used and the 2 PC's representing the NO and the Mobile terminal will communicate via TCP/IP.

The securing of cryptographic keys will be handled by the smart card, by access control mechanisms to the appropriate files and directories. In the PC representing the network, special protection measures for the secret keys are not appropriate in a demonstration environment. The keys used will be specific to the ASPeCT demonstrator and disclosure of them does not cause any threat to the demonstrated mechanisms. The UMTS authentication mechanism will be demonstrated using publicly available algorithms.

9.3.2 Software structure of the demonstration

A full description of the software structure for the ASPeCT demonstrator will be given in the design documentation. The OS used will be Windows for Workgroups 3.11 and as software development tool, the WATCOM C/C++ compiler is used.

Only the functionalities with regard to WP2.1 are explained here. Software blocks 9 and 10 contain only functionalities for WP2.3 and WP2.5 and are not explained here. All WP2.3 and WP2.5 functionalities of the software structure will be explained in document D07 [12].

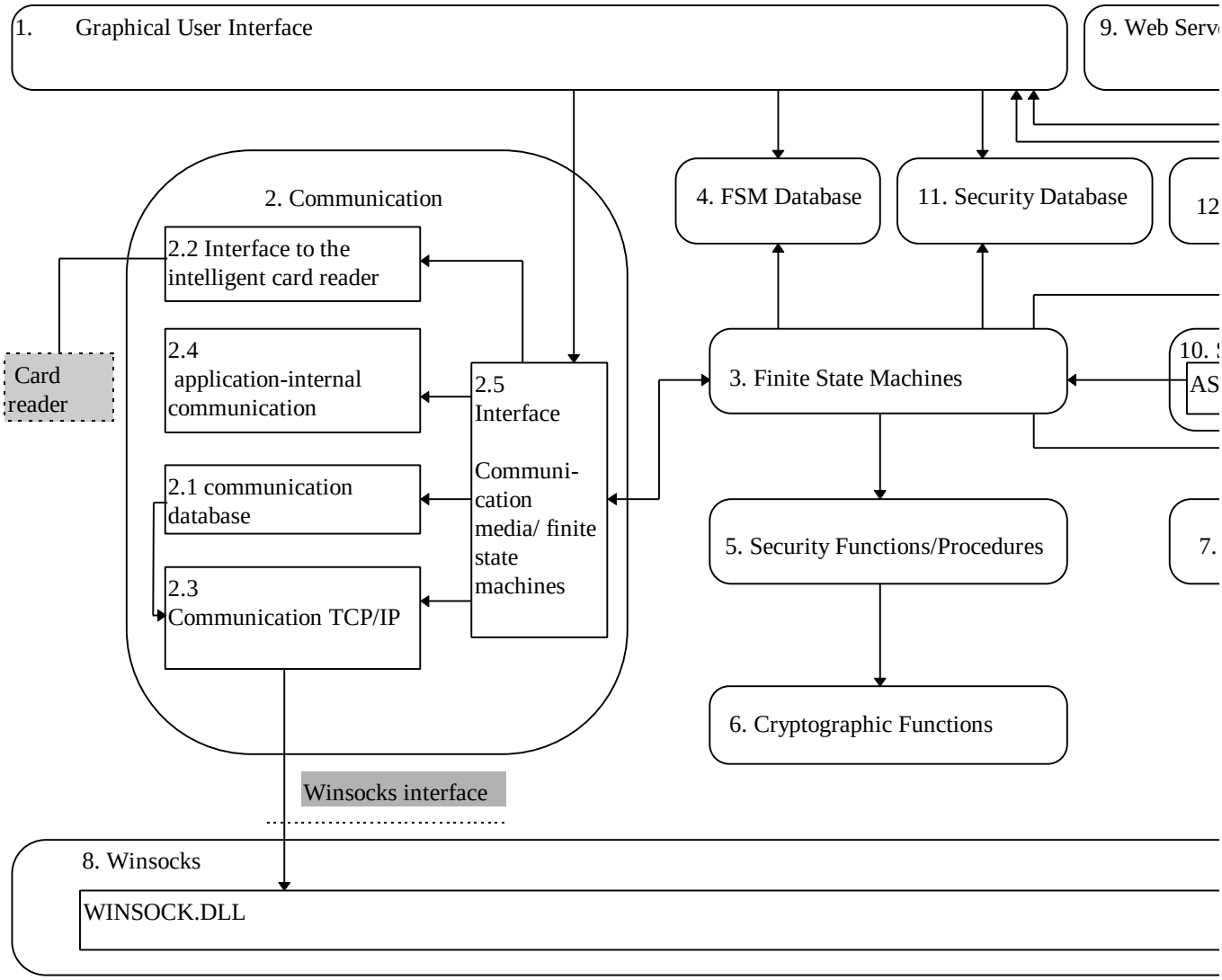


Figure 9-7 : Software Structure

This section describes each functional block in the software structure and the interfaces to other functional blocks.

9.3.2.1 Block 1 : GUI

This block contains different modules (a module is represented by a file), each module contains functions that may be used for one ore more of the other blocks in the software structure. Block 1 is not yet split up in different modules in this document.

The Graphical User Interface has following functionalities :

- The main application is defined in the GUI

- Administration of the communication database (See Section 9.3.2.2.5) :
    - creating a new entity with its address.
    - configuring the TCP/IP network.
    - activating the TCP/IP connections.

  This administration occurs via procedures defined in software block 2.1.

- When the user creates a new entity, then he has to indicate which Finite State Machine defined in block 3 corresponds to that new entity. The corresponding class will be instantiated and a reference to this instantiation is held in the communications database. When necessary, the user is requested to modify parameters specific for the created finite state machine. Parameters can be : types of security functions to be used, length of keys, etc...
  (See section 9.3.2.3 for a description of the finite state machines)

- Allows a user to start execution of a protocol via block 2.5.

- Allows the user to set tracepoints and levels of tracepoints before and during the tests or demonstrations. See Section 9.3.2.10 for a description of tracepoints.

- Offers procedures to the tracer (block 4) to open windows and display messages in them.

- It offers additional procedures to administer databases (e.g. block 11 : Security Database,) and to open windows and display messages in them (e.g. for block 4 : Tracer)

9.3.2.2 Block 2 : Communication

9.3.2.2.1 Block 2.1 : Communication database

This is a database containing all the data necessary for the communication.
This database holds a table with one entry for every entity in the configuration. Each entry in the table has following attributes :

- Name of the entity : e.g. TTP1 (Trusted Third Party), TTP2, IA1 (Interception Authority), IA2, SP1 (Service Provider), SP2, NO1 (Network Operator), NO2, VASP (Value Added Service Provider), MT (Mobile Terminal), IC1 (Intelligent Card reader), IC2.
  There is a predefined list of possible entity-names. This list must contain all the possible entities for all the workpackages.
- Number of the application that runs the entity. One or more applications may run on one or more PC's. Each application has a number. There is one server application and there may be 9 client applications.

- A reference to an instance of the finite state machine class.

When the user creates an entity then he has to indicate which Finite State Machine defined in block 3 corresponds to that new entity. The corresponding class will be instantiated and a reference to this instantiation is held in the communication database. When the application is not the server application in the network then a TCP/IP message will be sent to the server. This message will indicate the application number and new entity name. The server will update its database and send a similar message to all the other clients in the network, allowing them to update their database. One application may represent more than one entity. The communication database also makes use of procedures defined in block 2.3 to send messages to other TCP/IP nodes, as just mentioned.

9.3.2.2.2 Block 2.2 : Interface to the intelligent card reader

This block communicates to the serial port to which the intelligent card reader can be connected. The serial port communication is only used by the finite state machine simulating the Mobile Terminal. Block 2.2 has an interface to 2.5.

9.3.2.2.3 Block 2.3 : Communications TCP/IP

This block establishes the TCP/IP connections at initialisation phase and receives from and sends to the other PC's via TCP/IP.

9.3.2.2.4 Block 2.4 : Application-internal communication

This block is used when two entities run on the same application. There will be as good as no functionality in this block. The application sends a message to an own defined buffer.

9.3.2.2.5 Block 2.5 : Interface between the communication media and finite state machines

This block
- initialises the database on request from the GUI
- activates the TCP/IP connections on request from the GUI
- offers a common interface between the finite state machines created on the PC and the different communication media (serial, TCP/IP, internal).
- It accesses the communication database to get the entity (=finite state machine) attributes during protocol execution.
- It receives input from the GUI in order to activate one of the finite state machines.

This block also defines the abstract base class for a finite state machine which will be used by modules in block 3. In block 3 one derivation of the base class will be defined for each type of finite state machine. The base class will define a few basic functions e.g. ProcessIncomingMessage, which will handle incoming messages destined for the finite state machine.

9.3.2.3 Block 3 : Finite State Machines

This software block defines all the finite state machine classes. One instantiation of a finite state machine class represents one entity in the configuration. One application may represent one or more entities.
As explained in Sections 9.3.2.1 and 9.3.2.2.1 one of the available finite state machines is chosen for each entity running on the PC. This choice is made via the GUI.
At the same time, additional parameters may be set, like choice of algorithm, length of keys. Requirements on the GUI should be identified from the different workpackages. It is up to each

workpackage whether or not to define administerable parameters. Databases necessary to hold these parameters are defined in block 4.

Each workpackage in ASPeCT defines its own protocol machines, with states, databases.
Each finite state machine interprets the messages or events received from 2.5 and executes the corresponding protocol. It may send one or more messages via 2.5 and it goes to a new state.
The software interface between 2.5 and each defined finite state machine is common as mentioned in section 9.3.2.2.5.

A list of finite state machines (only those relevant for the migration demonstration are mentioned) is given hereafter, the functions achieved by the finite state machines are used:

- Authentication between the Mobile Terminal and the Network (Network operator and Service provider) in the Mobile Terminal
- Authentication between the Mobile Terminal and the Network in the Network Operator.
- Authentication between the Mobile Terminal and the Network in the Service Provider (may coincide with network operator)

9.3.2.4 Block 4 : FSM database

This block contains databases that hold parameters used in the finite state machines. These parameters can be written via the GUI.

9.3.2.5 Block 5 : Security Functions/Procedures

This block builds an ASPeCT specific interface towards basic cryptographic functions.

9.3.2.6 Block 6 : Cryptographic Functions

The basic cryptographic functions will be in this block.

9.3.2.7 Block 7 : ASN.1

This block contains C++ classes for ASN.1 definitions and procedures for encoding, decoding and displaying.

9.3.2.8 Block 8 : Winsocks

This block contains the standard Winsocks libraries.

9.3.2.9 Block 11 : Security Database

The security database holds parameters specific to the security layer and is administered via the GUI.

9.3.2.10 Block 12 : Tracer

The tracer can display messages on a screen or write them in a file. The tracer is configured via the GUI during initialisation of the demonstration. The finite state machines instruct the tracer to display or save messages.

Tracepoints are defined in the finite state machine. Each trace point has a level (1, 2, 3, ..). The user can define via the GUI which levels must be traced.

9.4 General Schedule

The schedule for the realisation of the demonstrator is done according the software engineering process model defined in the applicable quality procedures.

Phase	start-date	end-date	resulting document
Analysis	01/06/96	31/08/96	D5
Design	01/09/96	30/11/96	D12
Implementation	01/12/96	28/02/97	D12
Verification	01/03/97	31/05/97	D12

9.5 Effort

Following table shows the effort (in Manmonths) for each phase and each involved partner:

Phase	Vodafone	Panafon	Siemens Atea
Analysis			1,5
Design	1		2
Implementation			3
Verification		1	3

9.6 Test requirements

Tracing of the exchanged messages is necessary. Activation of tracepoints is thereby essential, different levels of tracing can be asked.

It has to be possible to introduce errors in the protocol, by changing the raw exchanged data.

All achieved goals of the protocols have to be visible, esp. the display of the negotiated cipher key.

Special attention has to be given to the test of error situations that could be caused by fraudulent access:

- Cloning of smartcards
- execute the protocol with the only goal to gain information on the user data or network data

10. Detailed specification of the demonstrator

This section will give a detailed specification of the demonstrator described in section 9.

It will specify the authentication protocols, the message contents, algorithms to be used ...

The messages are grouped according the procedures from the framework for authentication they belong to. Only messages from the following procedures will be used in the demonstrator:

- Procedure P1: user-NO authentication capability agreement
- Procedure P2: NO-SP authentication capability agreement
- Procedure P5: User-network authentication

10.1 Procedure P1: User-NO authentication capability agreement

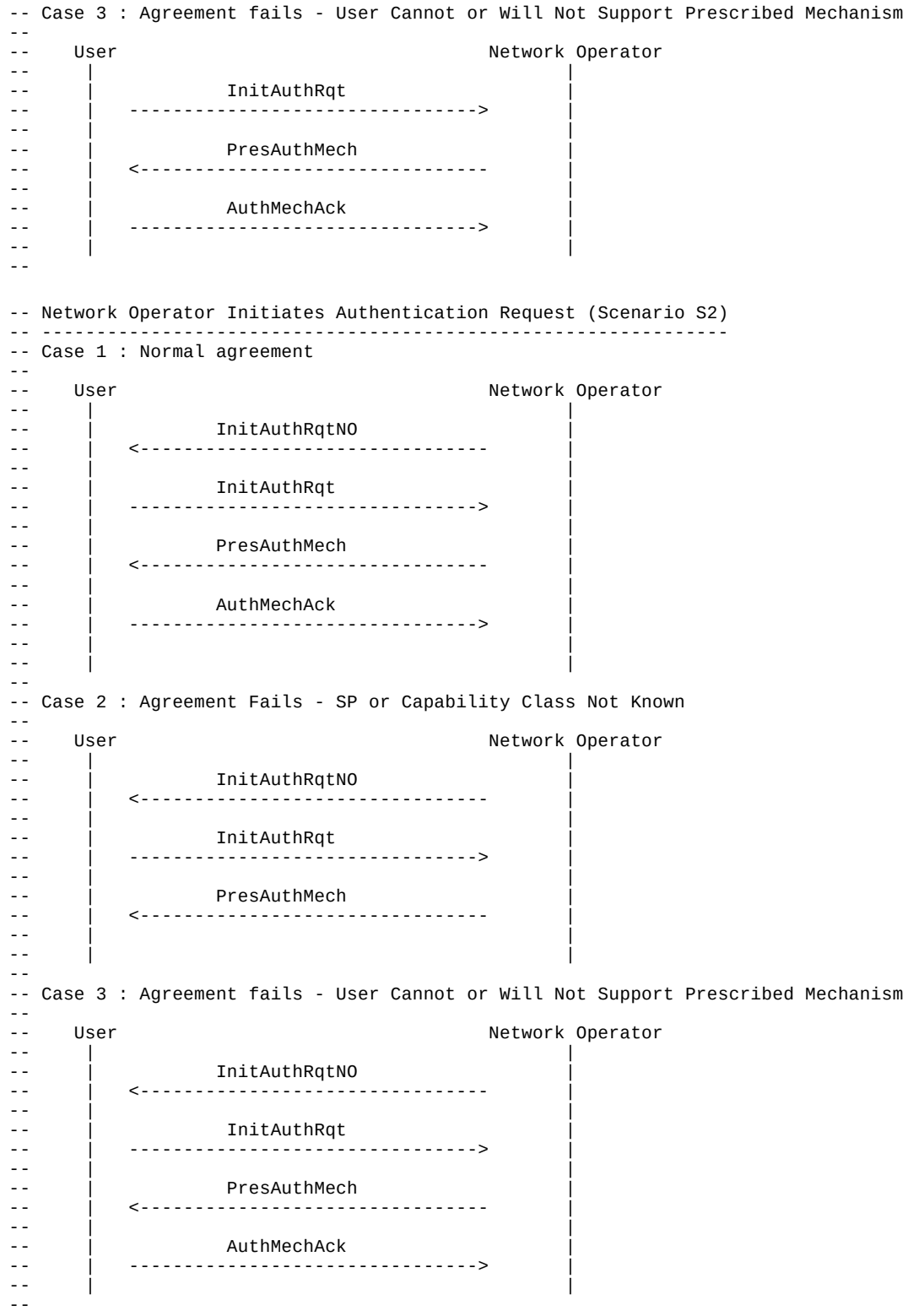
This is the Authentication Framework procedure which caters for requests for user-Network Operator authentication, prescription of authentication mechanism by the Network Operator and acknowledgement of the authentication mechanism by the user.

10.1.1 ASN.1 definitions of the exchanged messages

```
AuthenticationCapabilityU-NO DEFINITIONS ::=
BEGIN

  -- ****************************
  -- * Overview of the messages *
  -- ****************************

  CapabilityPDU ::= CHOICE
  {
    -- New Registrations: Roaming Agreement Exists (Scenario S1B)
    -- ----------------------------------------------------------
    -- Case 1 : Normal agreement
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |           InitAuthRqt                    |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |           PresAuthMech                   |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |           AuthMechAck                    |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |                                          |
    --
    -- Case 2 : Agreement Fails - SP or Capability Class Not Known
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |           InitAuthRqt                    |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |           PresAuthMech                   |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |                                          |
    --
```


-- Case 3 : Agreement fails - User Cannot or Will Not Support Prescribed Mechanism
--
--   User   Network Operator
-- | |
-- | InitAuthRqt |
-- | -------------------------------> |
-- | |
-- | PresAuthMech |
-- | <------------------------------- |
-- | |
-- | AuthMechAck |
-- | -------------------------------> |
-- | |
--
-- Network Operator Initiates Authentication Request (Scenario S2)
-- ---
-- Case 1 : Normal agreement
--
--   User   Network Operator
-- | |
-- | InitAuthRqtNO |
-- | <------------------------------- |
-- | |
-- | InitAuthRqt |
-- | -------------------------------> |
-- | |
-- | PresAuthMech |
-- | <------------------------------- |
-- | |
-- | AuthMechAck |
-- | -------------------------------> |
-- | |
-- | |
--
-- Case 2 : Agreement Fails - SP or Capability Class Not Known
--
--   User   Network Operator
-- | |
-- | InitAuthRqtNO |
-- | <------------------------------- |
-- | |
-- | InitAuthRqt |
-- | -------------------------------> |
-- | |
-- | PresAuthMech |
-- | <------------------------------- |
-- | |
-- | |
--
-- Case 3 : Agreement fails - User Cannot or Will Not Support Prescribed Mechanism
--
--   User   Network Operator
-- | |
-- | InitAuthRqtNO |
-- | <------------------------------- |
-- | |
-- | InitAuthRqt |
-- | -------------------------------> |
-- | |
-- | PresAuthMech |
-- | <------------------------------- |
-- | |
-- | AuthMechAck |
-- | -------------------------------> |
-- | |
--
InitAuthRqtNO [0] InitAuthRqtNO, -- Initiate Authentication Request, from Network
                                     Operator to user
InitAuthRqt   [1] InitAuthRqt,   -- Initiate Authentication Request, from user to
                                     Network Operator
PresAuthMech [2] PresAuthMech,   -- Prescribe Authentication Mechanism,
AuthMechAck   [3] AuthMechAck,   -- Acknowledge Authentication Mechanism,

```
  -- ***********************************************
  -- * Definition of the fields used in the messages *
  -- ***********************************************


  SPID      ::= OCTET STRING         -- Service Provider Identity
  NOID      ::= OCTET STRING         -- Network Operator Identity
  TUID      ::= OCTET STRING         -- Temporary User Identity
  CapClass  ::= OCTET STRING         -- Authentication Capability Class
  AuthMech  ::= OCTET STRING         -- Prescribed Authentication Mechanism
  MechAck   ::= INTEGER              -- Acknowledgement of Prescribed Mechanism

  -- ****************************************
  -- * Definition of the layout of the messages *
  -- ****************************************

  -- Initiate Authentication Request from Network Operator to User
  -- ------------------------------------------------------------------
  InitAuthRqtNO  ::= SEQUENCE
  {
    ****
  }

  -- Initiate Authentication Request from User to Network Operator
  -- ------------------------------------------------------------------
  InitAuthRqt  ::= SEQUENCE
  {
    ****
  }

  --  Prescribe Auhtentication Mechanism
  -- ------------------------------------------------------------------
  PresAuthMech ::= SEQUENCE
  {
    ****
  }

  --  Acknowledge Authentication Mechanism
  -- ------------------------------------------------------------------
  AuthMechAck  ::= SEQUENCE
  {
    ****
  }


END
```

10.1.2 Error handling

In addition to the above messages, there is a requirement for contingency messages to handle errors. Such errors will include *Network Operator Declines Authentication Request, Service Provider not known, Service Provider not reachable, Service Provider declines roaming agreement, Network operator declines roaming agreement* and *Service Provider declines authentication.*

10.2 Procedure P2: NO-SP authentication capability agreement

This is the Authentication Framework procedure which caters for requests by the Network Operator to the Service Provider for information on authentication capability class and for responses from the Service Provider to the Network Operator containing specifications of the particular authentication capability class.

10.2.1 ASN.1 definitions of the exchanged messages

```
AuthenticationCapabilityNO-SP DEFINITIONS ::=
BEGIN

  -- ***************************
  -- * Overview of the messages *
  -- ***************************

  CapabilityPDU ::= CHOICE
  {
    -- New Registrations: Roaming Agreement Exists (Scenario S1B)
    -- ----------------------------------------------------------
    -- Case 1 : Normal response
    --
    -- Network Operator                          Service Provider
    --      |                                           |
    --      |                CapsRqt                    |
    --      |   -------------------------------->       |
    --      |                                           |
    --      |                CapsInfo                   |
    --      |   <--------------------------------       |
    --      |                                           |
     --
    -- Case 2 : Response Fails - Capability Class Not Known
    --
    -- Network Operator                          Service Provider
    --      |                                           |
    --      |                CapsRqt                    |
    --      |   -------------------------------->       |
    --      |                                           |
    --      |                CapsInfo                   |
    --      |   <--------------------------------       |
    --      |                                           |
    --
    -- Case 3 : Response fails - Service Provider Will Not Supply Requested Data
    --
    -- Network Operator                          Service Provider
    --      |                                           |
    --      |                CapsRqt                    |
    --      |   -------------------------------->       |
    --      |                                           |
    --      |                CapsInfo                   |
    --      |   <--------------------------------       |
    --      |                                           |
    --

    CapsRqt [0] CapsRqt,  -- Request Information on Authentication Capability Class,
                          -- New Registrations: Roaming Agreement Exists
    CapsInfo[1] CapsInfo, -- Prescribe Authentication Mechanism,
                          -- New Registrations: Roaming Agreement Exists

    -- Network Operator Initiates Authentication Request (Scenario S2)
    -- ---------------------------------------------------------------
    -- Case 1 : Normal response
    --
    -- Network Operator                          Service Provider
    --      |                                           |
    --      |                CapsRqt                    |
    --      |   -------------------------------->       |
    --      |                                           |
    --      |                CapsInfo                   |
    --      |   <--------------------------------       |
    --      |                                           |
     --
```

```
    -- Case 2 : Response Fails - Capability Class Not Known
    --
    -- Network Operator                          Service Provider
    --      |                                          |
    --      |                CapsRqt                   |
    --      |   ------------------------------->       |
    --      |                                          |
    --      |                CapsInfo                  |
    --      |   <-------------------------------       |
    --      |                                          |
    --
    -- Case 3 : Response fails - Service Provider Will Not Supply Requested Data
    --
    -- Network Operator                          Service Provider
    --      |                                          |
    --      |                CapsRqt                   |
    --      |   ------------------------------->       |
    --      |                                          |
    --      |                CapsInfo                  |
    --      |   <-------------------------------       |
    --      |                                          |
    --

    CapsRqt [0] CapsRqt,  -- Request Information on Authentication Capability Class,
                          -- Network Operator Initiates Authentication Request
    CapsInfo[1] CapsInfo, -- Prescribe Authentication Mechanism,
                          -- Network Operator Initiates Authentication Request

  -- ***********************************************
  -- * Definition of the fields used in the messages *
  -- ***********************************************


  SPID      ::= OCTET STRING         -- Service Provider Identity
  NOID      ::= OCTET STRING         -- Network Operator Identity
  CapClass  ::= OCTET STRING         -- Authentication Capability Class

  -- ****************************************
  -- * Definition of the layout of the messages *
  -- ****************************************

  -- Authentication Request, New Registrations: Roaming Agreement Exists
  -- ------------------------------------------------------------------
  CapsRqt  ::= SEQUENCE
  {
    ****
  }

  -- Authentication Request, New Registrations: Roaming Agreement Exists
  -- ------------------------------------------------------------------
  CapsInfo ::= SEQUENCE
  {
    ****
  }

  -- Authentication Request, Network Operator Initiates Authentication Request
  -- -------------------------------------------------------------------------
  CapsRqt  ::= SEQUENCE
  {
    ****
  }

  -- Authentication Request, Network Operator Initiates Authentication Request
  -- -------------------------------------------------------------------------
  CapsRqt  ::= SEQUENCE
  {
    ****
  }

END
```

10.2.2 Error handling

In addition to the above messages, there is a requirement for contingency messages to handle errors. Such errors will include *Service Provider not known*, *Service Provider not reachable*, *Service Provider declines roaming agreement* and *Service Provider declines authentication.*

10.3 Procedure P5: User-network authentication

For the user-network authentication two mechanisms will be implemented, one using symmetric key techniques, the other using public key techniques. For both the mechanisms a protocol for Newly registered users and one for Currently registered users will be realised.

10.3.1 Taxonomy of the exchanged messages.

Following figure classifies the messages exchanged in the different authentication protocols. First, they are grouped according to the actual protocol. Within the protocol, they are grouped according to the communicating entities. The messages for error handling constitute a group of their own.

The numbers in the figure relate to the tags of the corresponding PDU's in the ASN.1 specification. Every authentication PDU has a unique tag. Strictly, it would only be necessary to have unique tags within one authentication protocol. This option was not taken. If, despite the protocol agreed, a party starts another protocol, this can be immediately recognised, without a need for putting an extra tag in the message, in order to identify the protocol.

Three spare tags (2, 3, 4) have been reserved for the introduction of new error messages.

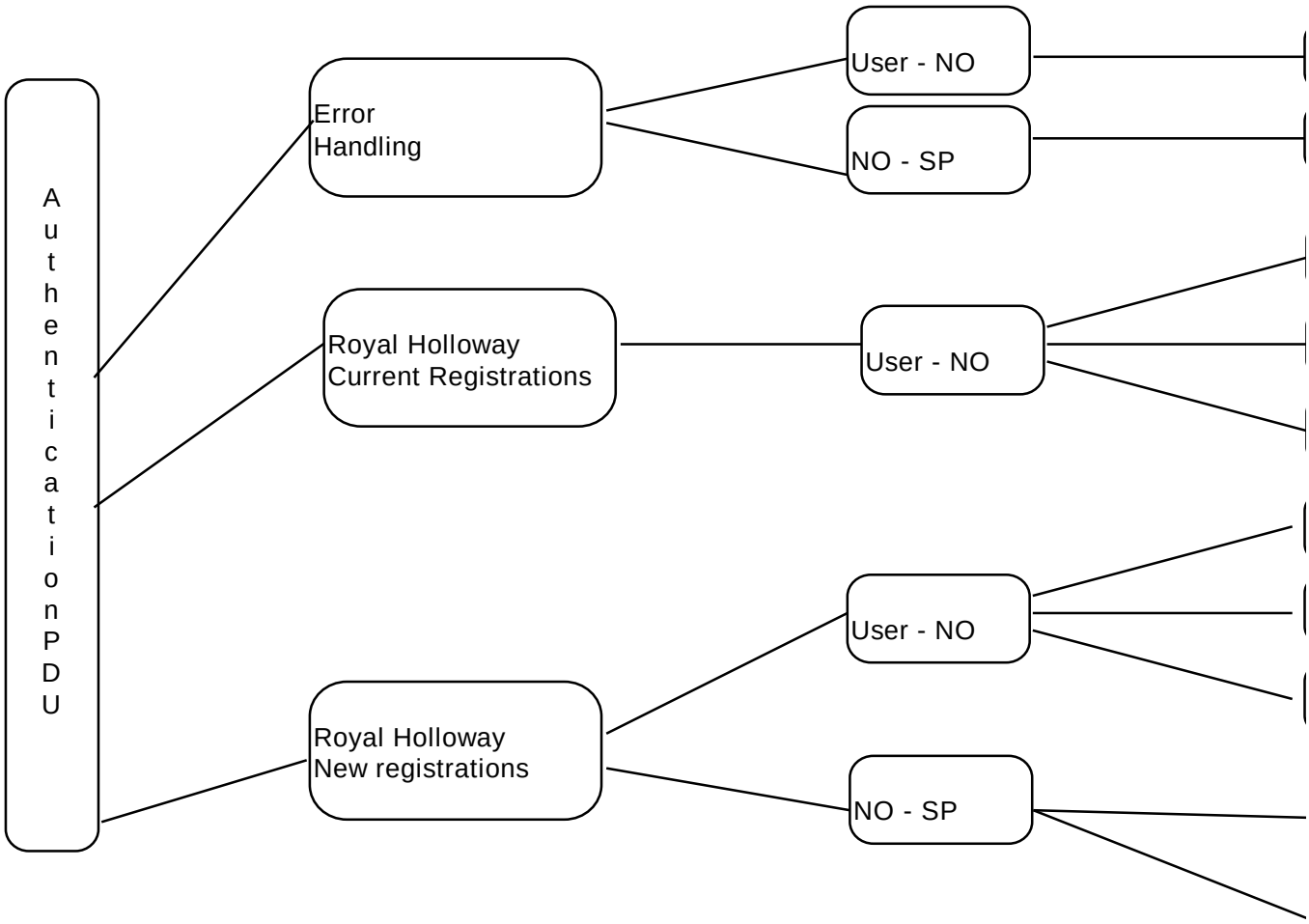


Figure 10-1 : Taxonomy of the exchanged messages

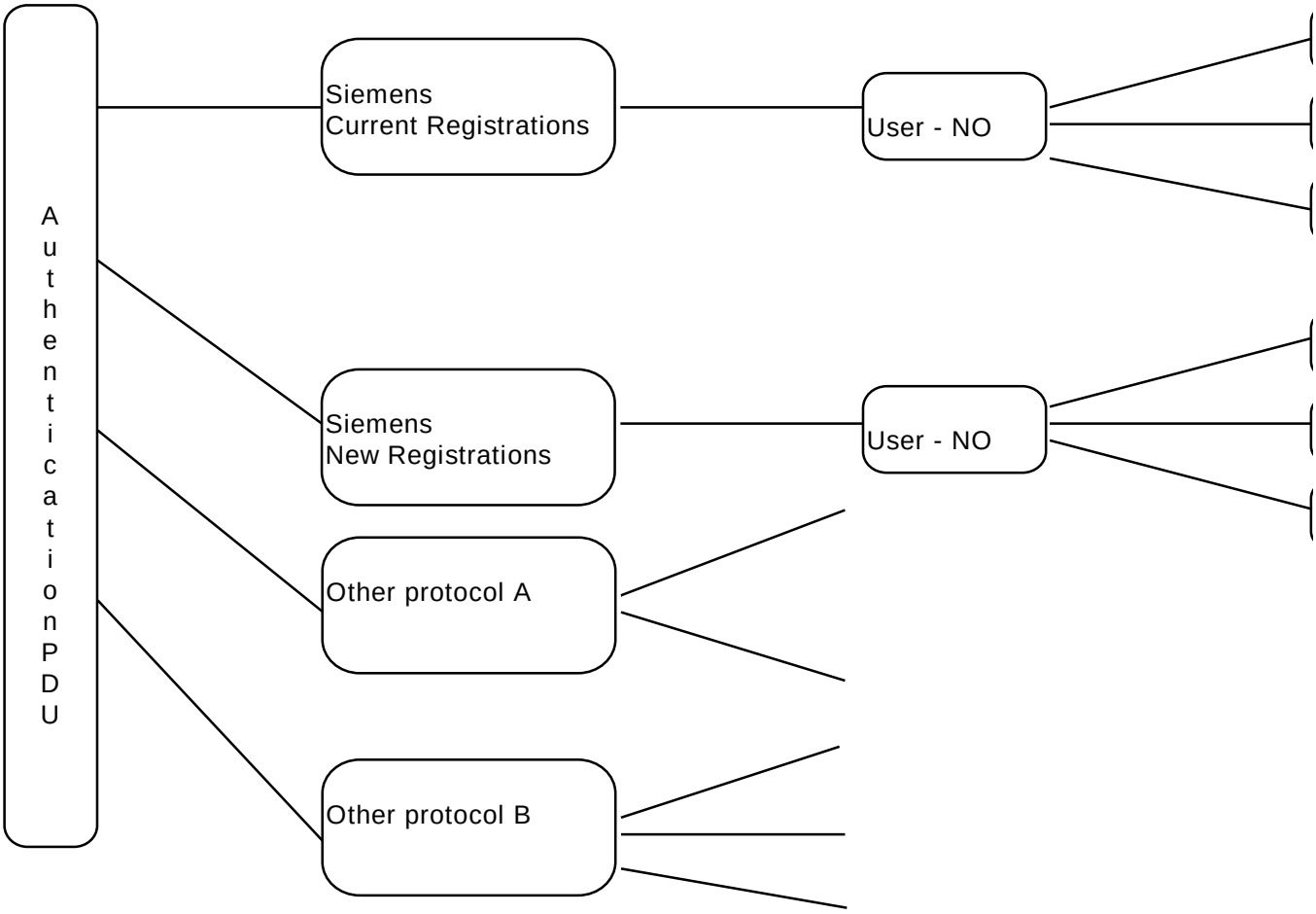


Figure 10-2 : Taxonomy of the exchanged messages - continued

10.3.2 ASN.1 definition of the exchanged messages

This chapter contains the ASN.1 definitions of the authentication PDU's. As much as possible, minimum and maximum sizes are added to the fields. The actual sizes depend on the underlying algorithms, which are still under discussion. The sizes should provide for enough storage capability, in order to support different kinds of algorithms for many years.

```
AuthenticationProtocol DEFINITIONS ::=
BEGIN

  -- ***************************
  -- * Overview of the messages *
  -- ***************************

  AuthenticationPDU ::= CHOICE
  {
    -- Royal Holloway Protocol, Current Registrations
    -- ----------------------------------------------
    -- Case 1 : Normal authentication
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |           authReqRhulCur                 |
    --     |   -------------------------------->      |
    --     |                                          |
    --     |           authContRhulCur                |
    --     |   <--------------------------------      |
    --     |                                          |
    --     |           authConfRhulCur                |
    --     |   -------------------------------->      |
    --     |                                          |
    --     |                                          |
    --
    -- Case 2 : Authentication of user fails
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |           authReqRhulCur                 |
    --     |   -------------------------------->      |
    --     |                                          |
    --     |           authContRhulCur                |
    --     |   <--------------------------------      |
    --     |                                          |
    --     |           authConfRhulCur                |
    --     |   -------------------------------->      |
    --     |                                          |
    --     |           authReject                     |
    --     |   <--------------------------------      |
    --     |                                          |
    --
    -- Case 3 : Authentication of network operator fails
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |           authReqRhulCur                 |
    --     |   -------------------------------->      |
    --     |                                          |
    --     |           authContRhulCur                |
    --     |   <--------------------------------      |
    --     |                                          |
    --     |           authReject                     |
    --     |   -------------------------------->      |
    --     |                                          |
    --
```

```
-- Case 4 : Network Operator does not know (or wants to know) user (TMUIn)
--
--    User                                  Network Operator
--     |                                          |
--     |           authReqRhulCur                 |
--     |   ------------------------------->       |
--     |                                          |
--     |           authReject                     |
--     |   <-------------------------------       |
--     |                                          |

authReqRhulCur  [5] AuthReqRhulCur,  -- Authentication Request,
                                     --   Current registration
authContRhulCur [6] AuthContRhulCur, -- Authentication Continue,
                                     --   Current registrations
authConfRhulCur [7] AuthConfRhulCur, -- Authentication Confirm,
                                     --   Current registrations

-- Royal Holloway Protocol, New Registrations
-- ------------------------------------------
-- Case 1 : Normal authentication
--
--    User                    Network Operator            Service Provider
--     |                          |                                  |
--     |      authReqRhulNew      |                                  |
--     |   -------------------->  |                                  |
--     |                          |                                  |
--     |                          |         authRegReq               |
--     |                          |   ---------------------------->  |
--     |                          |                                  |
--     |                          |         authRegConf              |
--     |                          |   <----------------------------  |
--     |                          |                                  |
--     |                          |                                  |
--     |      authContRhulNew     |                                  |
--     |   <--------------------  |                                  |
--     |                          |                                  |
--     |      authConfRhulNew     |                                  |
--     |   -------------------->  |                                  |
--     |                          |                                  |
--     |                          |                                  |
--
--
-- Case 2 : Service provider does not know, or does not want to know user
--
--    User                    Network Operator            Service Provider
--     |                          |                                  |
--     |      authReqRhulNew      |                                  |
--     |   -------------------->  |                                  |
--     |                          |                                  |
--     |                          |         authRegReq               |
--     |                          |   ---------------------------->  |
--     |                          |                                  |
--     |                          |         authRegRej               |
--     |                          |   <----------------------------  |
--     |                          |                                  |
--     |                          |                                  |
--     |      authReject          |                                  |
--     |   <--------------------  |                                  |
--     |                          |                                  |
--     |                          |                                  |
--
--
```

```
-- Case 3 : Authentication of network operator fails
--
--    User                    Network Operator             Service Provider
--     |                           |                                 |
--     |      authRegReq           |                                 |
--     |   -------------------->   |                                 |
--     |                           |                                 |
--     |                           |          authRegReq             |
--     |                           |   --------------------------->  |
--     |                           |                                 |
--     |                           |          authRegConf            |
--     |                           |   <---------------------------  |
--     |                           |                                 |
--     |                           |                                 |
--     |                           |                                 |
--     |      authContRhulNew      |                                 |
--     |   <--------------------   |                                 |
--     |                           |                                 |
--     |      authReject           |                                 |
--     |   -------------------->   |                                 |
--     |                           |                                 |
--     |                           |                                 |
--
-- Case 4 : Authentication of user fails
--
--    User                    Network Operator             Service Provider
--     |                           |                                 |
--     |      authReqRhulNew       |                                 |
--     |   -------------------->   |                                 |
--     |                           |                                 |
--     |                           |          authRegReq             |
--     |                           |   --------------------------->  |
--     |                           |                                 |
--     |                           |          authRegConf            |
--     |                           |   <---------------------------  |
--     |                           |                                 |
--     |                           |                                 |
--     |                           |                                 |
--     |      authContRhulNew      |                                 |
--     |   <--------------------   |                                 |
--     |                           |                                 |
--     |      authConfRhulNew      |                                 |
--     |   -------------------->   |                                 |
--     |                           |                                 |
--     |      authReject           |                                 |
--     |   <--------------------   |                                 |
--     |                           |                                 |
--     |                           |                                 |
--
-- Case 5 : Network Operator does not know, or does not want to know Service
--          Provider
--
--    User                    Network Operator             Service Provider
--     |                           |                                 |
--     |      authReqRhulNew       |                                 |
--     |   -------------------->   |                                 |
--     |                           |                                 |
--     |      authReject           |                                 |
--     |   <--------------------   |                                 |
--     |                           |                                 |
--     |                           |                                 |

authReqRhulNew  [8] AuthReqRhulNew,  -- Authentication Request new registrations
authContRhulNew [9] AuthContRhulNew, -- Authentication Continue new registrations
authConfRhulNew [10] AuthConfRhulNew, -- Authentication Confirm new registrations
authRegReq      [11] AuthRegReq,      -- Authentication Registration Request
authRegConf     [12] AuthRegConf,     -- Authentication Registration Confirm

-- If the Service Provider has no registration data for the user, he will
-- inform the network operator about it with an Authentication Registration
-- Reject

authRegRej     [2] AuthRegRej,       -- Authentication Registration Reject
```

```
    -- Siemens Current Registrations
    -- ------------------
    -- Case 1 : Normal authentication
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |            authReqSiemCur               |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authContSiemCur              |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |            authConfSiemCur              |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |                                          |
    --
    -- Case 2 : Authentication of User fails
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |            authReqSiemCur               |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authContSiemCur              |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |            authConfSiemCur              |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authReject                   |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |                                          |
    --
    -- Case 3 : Authentication of Network Operator fails
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |            authReqSiemCur               |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authContSiemCur              |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |            authReject                   |
    --     |   ------------------------------->      |
    --     |                                          |
    --

    authReqSiemCur   [13] AuthReqSiemCur,    -- Authentication Request Current
Registrations
    authContSiemCur  [14] AuthContSiemCur,   -- Authentication Continue Current
Registrations
    authConfSiemCur  [15] AuthConfSiemCur,   -- Authentication Confirm Current
Registrations

    -- Siemens New Registrations
    -- ------------------
    -- Case 1 : Successful authentication
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |            authReqSiemNew               |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authContSiemNew              |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |            authConfSiemNew              |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |                                          |
    --
```

```
    -- Case 2 : Authentication of User fails
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |            authReqSiemNew               |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authContSiemNew              |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |            authConfSiemNew              |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authReject                    |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |                                          |
    --
    -- Case 3 : Authentication of Network Operator fails
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |            authReqSiemNew               |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authContSiemNew              |
    --     |   <-------------------------------       |
    --     |                                          |
    --     |            authReject                    |
    --     |   ------------------------------->      |
    --
    -- Case 4 : Certification Authority not Known
    --
    --    User                                  Network Operator
    --     |                                          |
    --     |            authReqSiemCur               |
    --     |   ------------------------------->      |
    --     |                                          |
    --     |            authReject                    |
    --     |   <-------------------------------       |
    --     |                                          |

    authReqSiemNew   [16] AuthReqSiemNew,    -- Authentication Request, New
Registrations
    authContSiemNew  [17] AuthContSiemNew,   -- Authentication Continue, New
Registrations
    authConfSiemNew  [18] AuthConfSiemNew,   -- Authentication Confirm, New
Registrations

    -- Both Protocols, all unsuccessful cases
    -- --------------------------------------
    -- The authentication reject is used between User and Network operator,
    -- to flag the other party that his authentication has failed.

    authReject     [0] AuthReject       -- Authentication Reject
  }
```

```
-- ***********************************************
-- * Definition of the fields used in the messages *
-- ***********************************************


TmuiN     ::= SEQUENCE {           -- Temporary mobile user identity
                                   -- (Network operator <-> user)
                networkOperatorId  NoId, -- Identity of Network Operator
                userIdNO           UidNO -- Identity of User (assigned
                                         -- by the Network Operator)
              }
NoId      ::= OCTET STRING (SIZE (2..16))  -- Identity of Network Operator
UidNO     ::= OCTET STRING (SIZE (4..32)) -- User Identity (for NO)
TmuiS     ::= SEQUENCE             -- Temporary mobile user identity
              {                    -- (Service provider <-> user)
                serviceProviderId  SpId, -- Identity of Service Provider
                userIdSP           UidSP -- Identity of User (assigned
                                         -- by the Service Provider)
              }
SpId      ::= OCTET STRING (SIZE (2..16)) -- Identity of Service Provider
UidSP     ::= OCTET STRING (SIZE (4..32)) -- User Identity (for SP)
Random    ::= OCTET STRING (SIZE (8..32)) -- Random number for symmetrical
                                          -- algorithm
AuthN     ::= OCTET STRING (SIZE (8..32)) -- Authentication number
                                          -- (user -> network operator)
AuthS     ::= OCTET STRING (SIZE (8..32)) -- Authentication number
                                          -- (service provider -> user)
AuthU     ::= OCTET STRING (SIZE (8..32)) -- Authentication number
                                          --  (network operator to user)
EncTmuiN  ::= OCTET STRING (SIZE (6..42)) -- Encrypted Temporary mobile user
                                          -- identity TMUIN
EncTmuiS  ::= OCTET STRING (SIZE (6..40)) -- Encrypted Temporary mobile user
                                          -- identity TMUIS
KeyOffset ::= INTEGER                     -- Key offset
KeyNU     ::= OCTET STRING (SIZE (8..256)) -- Secret authentication key user -
                                           -- network operator
KeyAgreementValue ::= OCTET STRING        -- key agreement value
EncryptedData ::= OCTET STRING            -- Data encrypted using public key
IdCertAuth    ::= OCTET STRING (SIZE (2..16)) -- Identification of Certification
                                              -- authority
Certificate ::= OCTET STRING (SIZE (256..2200)) -- Certificate



-- ******************************************
-- * Definition of the layout of the messages *
-- ******************************************

-- Authentication Request, Royal Holloway, Current Registration
-- ------------------------------------------------------------
AuthReqRhulCur ::= SEQUENCE
{
  tmuin-old TmuiN,       -- Old Temporary Mobile User Identity, as known
                         -- to the network operator
  randu     Random       -- Random number, used as input of the
                         -- authentication algorithm by the Network Operator
}

-- Authentication Continue, Royal Holloway, Current Registration
-- -------------------------------------------------------------
AuthContRhulCur ::= SEQUENCE
{
  tmuin-new EncTmuiN,    -- Encrypted version of the new Temporary Mobile
                         -- User Identity, to be used in future communication
                         -- between user and network operator
  randn     Random,      -- Random number, used as input of the
                         -- authentication algorithm by user
  authn     AuthN        -- Output of the authentication algorithm calculated
                         -- by the Network operator
}

-- Authentication Confirm, Royal Holloway, Current Registration
-- ------------------------------------------------------------
AuthConfRhulCur ::= SEQUENCE
{
  authu     AuthU        -- Output of the authentication algorithm calculated
                         -- by the user
}
```

```
-- Authentication Request, Royal Holloway, New Registration
-- --------------------------------------------------------
AuthReqRhulNew ::= SEQUENCE
{
  tmuis-old TmuiS,       -- Old Temporary Mobile User Identity, as known
                         -- to the Service Provider
  randu     Random       -- Random number, used as input of the
                         -- authentication algorithm by network operator and
                         -- service provider
}

-- Authentication Continue, Royal Holloway, New Registration
-- ---------------------------------------------------------
AuthContRhulNew ::= SEQUENCE
{
  tmuis-new EncTmuiS,    -- Encrypted version of the new Temporary Mobile
                         -- User Identity, to be used in future communication
                         -- between user and service provider
  tmuin-new EncTmuiN,    -- Encrypted version of the new Temporary Mobile
                         -- User Identity, to be used in future communication
                         -- between user and network operator
  randn     Random,      -- Random number, used as input of the
                         -- authentication algorithm by user
  auths     AuthS,       -- Output of the authentication algorithm calculated
                         -- by the Service Provider
  authn     AuthN,       -- Output of the authentication algorithm calculated
                         -- by the Network operator
  keyOffset KeyOffset
}

-- Authentication Confirm, Royal Holloway, New Registration
-- --------------------------------------------------------
AuthConfRhulNew ::= SEQUENCE
{
  authu     AuthU        -- Output of the authentication algorithm calculated
                         -- by the user
}

-- Authentication Registration Request, Royal Holloway
-- ---------------------------------------------------
AuthRegReq ::= SEQUENCE
{
  tmuis-old TmuiS,       -- Old Temporary Mobile User Identity, as known
                         -- to the Service Provider
  randu     Random       -- Random number, used as input of the
                         -- authentication algorithm by the service provider
}

-- Authentication Registration Confirm, Royal Holloway
-- ---------------------------------------------------
AuthRegConf ::= SEQUENCE
{
  tmuis-new EncTmuiS,    -- Encrypted version of the new Temporary Mobile
                         -- User Identity, to be used in future communication
                         -- between user and service provider
  auths     AuthS,       -- Output of the authentication algorithm calculated
                         -- by the Service Provider
  keyOffset KeyOffset,   -- Key offset, used for calculation of secret
                         -- authentication key (for authentication between
                         -- user and network operator)
  keyNU     KeyNU        -- Secret authentication key, to be used between
                         -- User and Network Operator
}

-- Authentication Request, Siemens, Current Registrations
-- ------------------------------------------
AuthReqSiemCur ::= SEQUENCE
{
  keyAgreementValue KeyAgreementValue  -- Value for network operator to
                                       -- base key agreement upon
}
```

```
  -- Authentication Confirm, Siemens, Current Registrations
  -- ------------------------------------------
  AuthContSiemCur ::= SEQUENCE
  {
    randn     Random,       -- Value for user to base key agreement upon
    authn     AuthN,        -- Value of network operator, used to authenticate
                            -- him to the user
    encData1  EncryptedData -- Encrypted data (data1), to be decrypted and
                            -- signed by the user
  }

  -- Authentication Continue, Siemens, Current Registrations
  -- ------------------------------------------
  AuthConfSiemCur ::= SEQUENCE
  {
    encSign   EncryptedData, -- Signature on session key, data received
                             -- from network operator (data1) and user
                             -- generated data (data2)
    encImui   EncryptedData, -- Encrypted International Mobile User Identity
    encData2  EncryptedData  -- Encrypted data2
  }

  -- Authentication Request, Siemens, New Registrations
  -- ------------------------------------------
  AuthReqSiemNew ::= SEQUENCE
  {
    keyAgreementValue KeyAgreementValue, -- Value for network operator to
                                         -- base key agreement upon
    idCertAuth        IdCertAuth         -- Identity of certification
                                         -- authority
  }

  -- Authentication Continue, Siemens, New Registrations
  -- ------------------------------------------
  AuthContSiemNew ::= SEQUENCE
  {
    randn     Random,        -- Value for user to base key agreement upon
    authn     AuthN,         -- Value of network operator, used to authenticate
                             -- him to the user
    encData1  EncryptedData, -- Encrypted data (data1), to be decrypted and
                             -- signed by the user
    certN     Certificate    -- Network Operator Certificate
  }

  -- Authentication Confirm, Siemens, New Registrations
  -- ------------------------------------------
  AuthConfSiemNew ::= SEQUENCE
  {
    encSign   EncryptedData, -- Signature on session key, data received
                             -- from network operator (data1) and user
                             -- generated data (data2)
    encCertU  EncryptedData, -- User Certificate
    encData2  EncryptedData  -- Encrypted data2
  }

  -- Both messages for flagging error conditions to the other party,
  -- do not contain any indication what exactly went wrong (like user not
  -- known, bad authentication data calculated and so on).  The principle
  -- behind it is, if authentication fails, the (possible) intruder must not
  -- be given any indication what exactly went wrong.

  -- Authentication Reject
  -- ------------------------
  AuthReject ::= NULL

  -- Authentication Registration Reject, Royal Holloway
  -- ------------------------------------------------
  AuthRegRej ::= NULL

END
```

10.3.3 Certificate format

The ASPeCT certificate format proposed in D07 will be used. It is briefly explained below. Refer to D07 for a more thorough discussion.

10.3.3.1 The Certificate Information Sequence

A certificate contains two kinds of information. The data needed for establishing a secure communication channel with some party (i.e. the certificate information sequence) and the proof that this data can be trusted (i.e. a signature from the Certification Authority).

Field	Contents	Description	Length
1.	Map field	This field gives the map which fields and options will be presented in the certificate. It includes the following 8-bit information: 1 public key (1) / secret key (0) 2 issuer public key identifier present (1) / not present (0) 3 issuer identifier format: hash (1) / plain (0) 4 subject private key usage period present (1) / not present (0) 5 subject identifier format: hash (1) / plain (0) 6 subject key usage present (1) / not present (0) 7 cross certificate attribute present (1) / not present (0) 8 certification path present (1) / not present (0)	1 byte binary
2.	Version	The version number of the certificate. The version that we will start with is V1.0 This field will therefore contain the value 10 (hex).	1 byte binary
3.	Serial Number	Unique number of the certificate, assigned by the issuer.	12 bytes ASCII
4.	Public key identifier	Optional. Unique identifier of the public key (e.g., as key updating occurs) to be used to verify the signature on this certificate.	1 byte binary
5.	Issuer Identifier	There are two options for the issuer identifier: 1 the hashed issuer identifier, 2 the plain issuer identifier.	 16 bytes binary 15 + 30 bytes ASCII
1	Validity	Including four dates: 1 the date before the certificate is not valid, 2 the date after the certificate is no longer valid. 3 optional private key usage period: including the date before and the date after as well. It is used when the subject private key usage period is not the same as the public key validity.	 6 byte ASCII 6 byte ASCII 6 + 6 bytes ASCII
2	Subject Identifier	There are two options for the subject identifier: 1 the hashed subject identifier, 2 the plain subject identifier.	 16 bytes binary 15 + 30 bytes ASCII
3	Subject key usage	Optional. The usage of the subject key being certified includes: 1 digital signature, 2 data encryption, 3 key agreement, 4 key certificate signature, 5 CRL signature.	1 nibble binary 0 1 2 3 4
4	Cross certificate attributes	Optional. Two situations: 1 The public key certified will be used to sign another certificate (issuer identity and certificate serial number). 2 The public key used to signed this certificate was certified by another certificate (issuer identity and certificate serial number).	 30 byte binary 30 byte binary
5	Certificate path attributes	Optional. Two subfields: 1 Path length - the number of related certificates. 2 A list of subject identifiers included in the certificate path.	 1 byte binary 16 byte binary per each subject name
6	Subject	An algorithm identifier plus a public key value for the subject.	

	public key information	Subfield 1: algorithm identifier 0 = RSA 1 = elliptic curve 2 = Diffie-Hellman other unspecified	1 byte binary
		If algorithm identifier = 0	
		Subfield 2: modulus length of key in bits	2 bytes binary
		Subfield 3: exponent length of key in bits	2 bytes binary
		Subfield 4: key value: first modulus, then exponent of key	sum of values of subfields 2 and 3 bytes binary
		If algorithm identifier = 1	
		Subfield 2: length of x-coordinate of key	2 bytes binary
		Subfield 3: length of y-coordinate of key	2 bytes binary
		Subfield 4: key value: first x-coordinate, then y-coordinate of key	sum of values of subfields 2 and 3 bytes binary
		If algorithm identifier = 2	
		Subfield 2: modulus (p) length of key in bits	2 bytes binary
		Subfield 3: root (g) length of key in bits	2 bytes binary
		Subfield 4: value (gx mod p) length of key in bits	2 bytes binary
		Subfield 5: key value: p, g, gx mod p	sum of values of subfields 2, 3 and 4 bytes binary

Table 10-1 shows the contents of the certificate information sequence.

Field	Contents	Description	Length
1.	Map field	This field gives the map which fields and options will be presented in the certificate. It includes the following 8-bit information: 1 public key (1) / secret key (0) 2 issuer public key identifier present (1) / not present (0) 3 issuer identifier format: hash (1) / plain (0) 4 subject private key usage period present (1) / not present (0) 5 subject identifier format: hash (1) / plain (0) 6 subject key usage present (1) / not present (0) 7 cross certificate attribute present (1) / not present (0) 8 certification path present (1) / not present (0)	1 byte binary
2.	Version	The version number of the certificate. The version that we will start with is V1.0 This field will therefore contain the value 10 (hex).	1 byte binary
3.	Serial Number	Unique number of the certificate, assigned by the issuer.	12 bytes ASCII
4.	Public key identifier	Optional. Unique identifier of the public key (e.g., as key updating occurs) to be used to verify the signature on this certificate.	1 byte binary
5.	Issuer Identifier	There are two options for the issuer identifier: 1 the hashed issuer identifier, 2 the plain issuer identifier.	 16 bytes binary 15 + 30 bytes ASCII
1	Validity	Including four dates: 1 the date before the certificate is not valid, 2 the date after the certificate is no longer valid. 3 optional private key usage period: including the date before and the date after as well. It is used when the subject private key usage period is not the same as the public key validity.	 6 byte ASCII 6 byte ASCII 6 + 6 bytes ASCII

2	Subject Identifier	There are two options for the subject identifier: 1 the hashed subject identifier, 2 the plain subject identifier.	 16 bytes binary 15 + 30 bytes ASCII
3	Subject key usage	Optional. The usage of the subject key being certified includes: 1 digital signature, 2 data encryption, 3 key agreement, 4 key certificate signature, 5 CRL signature.	1 nibble binary 0 1 2 3 4
4	Cross certificate attributes	Optional. Two situations: 1 The public key certified will be used to sign another certificate (issuer identity and certificate serial number). 2 The public key used to signed this certificate was certified by another certificate (issuer identity and certificate serial number).	 30 byte binary 30 byte binary
5	Certificate path attributes	Optional. Two subfields: 1 Path length - the number of related certificates. 2 A list of subject identifiers included in the certificate path.	 1 byte binary 16 byte binary per each subject name
6	Subject public key information	An algorithm identifier plus a public key value for the subject. Subfield 1: algorithm identifier 0 = RSA 1 = elliptic curve 2 = Diffie-Hellman other unspecified If algorithm identifier = 0 Subfield 2: modulus length of key in bits Subfield 3: exponent length of key in bits Subfield 4: key value: first modulus, then exponent of key If algorithm identifier = 1 Subfield 2: length of x-coordinate of key Subfield 3: length of y-coordinate of key Subfield 4: key value: first x-coordinate, then y-coordinate of key If algorithm identifier = 2 Subfield 2: modulus (p) length of key in bits Subfield 3: root (g) length of key in bits Subfield 4: value (g^x mod p) length of key in bits Subfield 5: key value: p, g, g^x mod p	 1 byte binary 2 bytes binary 2 bytes binary sum of values of subfields 2 and 3 bytes binary 2 bytes binary 2 bytes binary sum of values of subfields 2 and 3 bytes binary 2 bytes binary 2 bytes binary 2 bytes binary sum of values of subfields 2, 3 and 4 bytes binary

Table 10-1 : Certificate Information Sequence Format

10.3.3.2 Signatures on the Certificate Information Sequence

The certificate information sequence must be signed. ASPeCT has two models of signatures for certificate information sequences : RSA and AMV signatures. RSA signatures can be subdivided in two subtypes.

10.3.3.2.1 RSA Signatures

If the certificate information sequence M is short enough, a check code H is calculated. M and H are transformed in a string S_r. It is possible to reestablish M and H from S_r without requiring other data. The signature is $Sign_s(S_r) = S_r^s \bmod n$.

If the certificate information sequence M is too long for applying the previous method, a hash code H' is calculated over the entire message M. Then M is split into two parts : M_x and M_r. M_r and H' are used for creation of a string S_r'. The signature is $Sign(S_r') = S_r'^s \bmod n$.

This results in one of the two formats for RSA-signatures in Table 10-2. (k is the length of the modulus in bits, x is the length of M_x in bytes).

Type of Certificate one bit	*Signature* *k* bits	*Non-recoverable data* *8x* bits
0	$Sign_s(S_r)$	
0	$Sign_s(S_r')$	M_x

Table 10-2 : Certificate format based on RSA-signature

10.3.3.2.2 AMV signatures

The AMV signature is an ELGamal type signature scheme based on elliptic curves over finite fields. A finite commutative group and a parameter p, divisor of the cardinality of this group, must be chosen. The signature consists of two parts R and S. The resulting certificate format is given in Table 10-3. The length of the appendix depends a.o. on the length of the parameter p.

Type of certificate one bit	Certificate information sequence m bits	Appendix 256 bits
1	M	R,S

Table 10-3 : Certificate format based on AMV-signature

10.3.4 Length estimations of the different messages

This chapter tries to give an estimation of the length of the messages used in the different protocols. The lengths of the parameters are all educated estimations. As a consequence, the lengths of the messages are also estimations. Please use these numbers with care, they are subject to change. Better estimations will be possible, after all algorithms to be used have been defined.
The length of messages is influenced by two factors : the length of the actual data in the fields, and the way the fields are represented. An overhead of 2 bytes per message and of 2 bytes per field in the message is calculated (tag + length specifier).
All lengths are specified in bytes.
The authReject and authRegReject messages are not mentioned, because they do not carry any data fields (as conceived at this moment).

10.3.4.1 Royal Holloway Protocol

Field	authReqRhulCur	authContRhulCur	authConfRhulCur
tmuin-old	8		
randu	16		
tmuin-new		8	
randn		16	
authn		20	20
authu			
Total fields	24	44	20
ASN.1 Encoding	6	8	4
Total	30	52	24

Table 10-4 Message lengths Current Registration: Symmetric key authentication

Field	authReqRhulNew	authContRhulNew	authConfRhulNew
tmuis-old	8		
randu	16		
tmuin-new		8	
tmuis-new		8	
randn		16	
auths		20	
authn		20	
authu			20
keyOffset		4	
Total fields	24	76	20
ASN.1 Encoding	6	14	4
Total	30	90	24

Table 10-5 Message lengths New Registration: Symmetric key authentication

Field	authRegReq	authRegConf
tmuis-old	8	
randu	16	
tmuis-new		8
auths		20
keyNU		24
keyOffset		4
Total fields	24	56
ASN.1 Encoding	6	10
Total	30	66

Table 10-6 Message lengths New Registration: Symmetric key authentication (NO-SP messages)

10.3.4.2 Siemens Protocol

The Siemens Protocol allows data to be exchanged during the authentication protocol. These data, to realise the non-repudiation feature, is not counted in the estimations.
The field lengths needed will depend a.o. on the key agreement mechanism used (finite field GF(p), elliptic curves, ...). A mechanism based on a finite field GF(p) is considered to be the worst case scenario (as far as field lengths are concerned).

The introduction of temporary identities into this protocol will influence the message lengths. The Request and Continue messages may grow with about 10 bytes.

For some fields, the tables contain two numbers : a pessimistic and an optimistic one.

The pessimistic estimate of the length of the certificate is made as follows. If all fields are present in the certificate information sequence, and if both modulus and exponent of the certified public key are 768 bits long, the length of the certificate information sequence is about 400 bytes. Suppose a 1024 bit RSA mechanism is used for signing the certificate (1024 bit = 128 bytes). Suppose RIPEMD-160 is used as has algorithm, producing a 20 bytes hash value. Then about 100 bytes can be combined with the 20 byte hash value, for generation of the signature. This results in 128 bytes. The 300 remaining bytes of the certificate information sequence must be added to the certificate, giving a total of 128+300 bytes = 428 bytes. Rounding up to the nearest multiple of 50 gives 450 bytes.

The optimistic estimate of the length of the certificate is made as follows. No optional fields are present in the certificate information sequence. A 160 bit elliptic curve is used for the user signature, limiting the length of the field “subject public key info” to 45 bytes. The length of the certificate information sequence then becomes 103 bytes. If a 1024 bit RSA signature with message recovery is put upon it, the certificate information sequence completely fits within the 1024 bit block. This reduces the total certificate length to 128 bytes.

Field	authReqSiemCur	authContSiemCur	authConfSiemCur
keyAgreementValue	96 / 40		
randn		8	
authn		8	
encData1		0	
encSign			96 / 40
encImui			8
encData2			0
Total fields	96 / 40	16	104 / 48
ASN.1 Encoding	4	8	8
Total	100 / 44	24	112 / 45

Table 10-7 Message lengths Current Registration: Public key authentication

Field	authReqSiemNew	authContSiemNew	authConfSiemNew
keyAgreementValue	96 / 40		
idCertAuth	4		
randn		8	
authn		8	
encData1		0	
certN		450 / 128	
encSign			96 / 40
encCertU			450 / 128
encData2			0
Total fields	100 / 44	466 / 144	546 / 168
ASN.1 Encoding	6	10	8
Total	106 / 50	476 / 154	554 / 176

Table 10-8 Message lengths New Registration: Public key authentication

10.3.5 Error handling

If one party authenticates another party, that authentication may fail. Two reactions are possible : the other party is informed about the failed authentication, or the other party is not informed about it.

If it is certain that if authentication fails, the other party is an intruder, just ignoring that other party might be a good enough reaction. However, also the authentication of a legitimate party may fail. In that case, it would be very rude not to inform it, why the connection could not be established.

The solution for handling authentication failures in the above protocols, takes an intermediate approach : if authentication fails, it is reported, but in a message without any parameters. A possible intruder can not derive the exact reason for the authentication failure from it. He is not given any extra information, that might allow him to figure out another way for intruding. A legitimate party knows something is wrong with the authentication and knows he must take action accordingly.

When an authentication fails, everything must be restored to the state it was in before authentication started. An intruder should not disable the legitimate party to establish a connection, because (e.g.) the TMUIN changed during a (failed) authentication attempt. That is, on reception of an authReject message, fields that were updated during the authentication procedure, must be restored to the value they had before authentication began.

The protocol does not take into account the loss of authReject messages, nor does it handle the case of "ghost" authReject messages (i.e. authReject messages arriving from an unknown source). As most authentications will be successful, this will almost never lead to real problems.

10.3.6 Specification of the algorithms

The abbreviations between brackets in the subtitles correspond with the notations of AC095/ATEA/W21/DS/P/02/B.2 "Initial Report on Security Requirements" chapter 7.3.

10.3.6.1 Algorithms Used in the RHUL protocol

10.3.6.1.1 Symmetrical user authentication algorithm (A_U)

Purpose :	Authentication of user towards Network Operator using symmetrical algorithm
Who :	User and network operator
When :	User, for generating authu field sent in AuthConfRhulCur and AuthConfRhulNew messages Network operator, for checking authu field received in AuthConfRhulCur and AuthConfRhulNew messages
Input :	Random number randn : size to be defined Random number randu : size to be defined Secret key keyNU : size to be defined
Output :	Authentication parameter authu : size to be defined
Algorithm :	to be specified; will probably be based on some kind of hash algorithm (e.g. RIPE-MD)

10.3.6.1.2 Symmetrical network operator authentication algorithm (A_U)

Purpose : Authentication of Network Operator towards User using symmetrical algorithm
Who : User and network operator
When : User, for checking authn field sent in AuthContRhulCur and AuthConfRhulNew messages
Network operator, for generating authn field sent in AuthContRhulCur and AuthContRhulNew messages
Input : Random number randu : size to be defined
Random number randn : size to be defined
Secret key keyNU : size to be defined
Decrypted tmuin-new : size to be defined
Output : Authentication parameter authn : size to be defined
Algorithm : to be specified
The basis of the algorithm is the same as for the symmetrical user authentication algorithm. The main difference is the extra input parameter tmuin-new.

10.3.6.1.3 Symmetrical Service Provider authentication algorithm (A_S)

Purpose : Authentication of Service Provider towards User using symmetrical algorithm
Who : User and Service Provider
When : User, for checking auths field sent in AuthContRhulNew messages
Service Provider, for generating auths field sent in AuthRegConf message
Input : Random number randu : size to be defined
Secret key keySU : size to be defined
tmuis-new : size to be defined
Output : Authentication parameter auths : size to be defined
Algorithm : to be specified . Will probably be based on some kind of hash algorithm (e.g. RIPEMD).

10.3.6.1.4 TMUIn cipher key generator (C_U)

Purpose : Generation of encryption key CIPHn, used to encrypt TMUIn in AuthContRhulCur and AuthContRhulNew messages
Who : User and Network Operator
When : User, before decrypting the encrypted tmuin-new
Network Operator : before encrypting tmuin-new
Input : Random number randu : size to be defined
Secret key keyNU : size to be defined
Output : Cipher key CIPHn : size equal to size of tmuin
Algorithm : to be specified . Will probably be based on some kind of hash algorithm (e.g. RIPEMD).

10.3.6.1.5 TMUIn encryption/decryption algorithm

Purpose : Encryption of tmuin-new for transfer from network operator to user
Who : User and Network Operator
When : User, when decrypting the encrypted tmuin-new
Network Operator : for encrypting tmuin-new
Input : plain tmuin-new : size to be defined
Cipher key CIPHN : size equal to the size of tmuin
Output : encrypted tmuin-new : size equal to the size of tmuin
Algorithm : Exclusive or of plain tmuin-new and CIPHN

10.3.6.1.6 TMUIs cipher key generator (C_U)

Purpose : Generation of encryption key CIPHs, used to encrypt TMUIs in AuthRegConf and AuthContRhulNew messages
Who : User and Service Provider
When : User, before decrypting the encrypted tmuis-new
Service Provider : before encrypting tmuis-new
Input : Random number randu : size to be defined
Secret key keySU : size to be defined
keyOffset : range to be defined
Output : Cipher key CIPHs : size equal to size of tmuis
Algorithm : to be specified
The basis of the algorithm is the same as for the TMUIn cipher key generator. The main difference is the extra input parameter keyOffset and the parameter keySU that replaces keyNU.

10.3.6.1.7 TMUIs encryption/decryption algorithm

Purpose : Encryption of tmuis-new for transfer from network operator to user
Who : User and Service Provider
When : User, when decrypting the encrypted tmuis-new
Service Provider, for encrypting tmuis-new
Input : plain tmuis-new : size to be defined
Cipher key CIPHs : size equal to the size of tmuis
Output : encrypted tmuis-new : size equal to the size of tmuis
Algorithm : Exclusive or of plain tmuis-new and CIPHs

10.3.6.1.8 keyNU Generator (A_N)

Purpose : Generation of new secret key keyNU, to be used between Network operator and User
Who : User and Service Provider
When : User, when receiving AuthContRhulNew message
Service Provider, when composing AuthRegConf message
Input : secret key keySU : size to be defined
network operator ID : size to be defined (by who ?)
keyOffset : range to be defined
Output : keyNU : size equal to be defined
Algorithm : to be specified . Will probably be based on some kind of hash algorithm (e.g. RIPEMD).

10.3.6.2 Algorithms Used in the Siemens protocol

10.3.6.2.1 Symmetric Encryption Algorithm (Enc)

Purpose : Encryption of data
Who : User and Network Operator
When : Confidentiality between User and Network Operator
Input : secret key Ks : size to be defined
data : size variable
Output : encrypted data
Remark : Because the size of the input data is variable, the algorithm must provide some mechanism to allow his decryption counterpart to restore the length of the original data
Algorithm : to be specified

10.3.6.2.2 Symmetric Decryption Algorithm (Dec)

Purpose : Decryption of data
Who : User and Network Operator
When : Confidentiality between User and Network Operator
Input : secret key Ks : size to be defined
encrypted data : size variable
Output : plain data : size variable
Remark : Because the size of both encrypted and plain data is variable, the algorithm must provide some mechanism for restoring the length of the original plain text data
Algorithm : to be specified . It must correspond to the symmetric Encryption Algorithm

10.3.6.2.3 Finite group for Key Agreement

The finite group to be used for key agreement must be defined. Any group in which the discrete logarithm problem is hard will do. It must be defined what exponentiation in this group means.(To be provided by Siemens).

10.3.6.2.4 Symmetrical key agreement algorithm (h1)

Who : User and Network Operator
When : During authentication
Input : element of finite group for Key Agreement
random number : size to be defined
Output : secret key Ks : size to be defined
Algorithm : to be specified

10.3.6.2.5 Hash function for key confirmation (h2)

Who : User and Network Operator
Purpose : To verify correctness of secret symmetrical key, calculated independently by both sides.
When : During key agreement
Input : Secret key Ks (data to be defined)
Output : Confirmation value Authn : size to be defined
Algorithm : To be specified

10.3.6.2.6 Hash function for signature generation (h3)

Who : User and Network Operator
Purpose : To convert data of variable size into a hash value of fixed size.
When : During signature calculation/verification
Input : Data of variable size
Output : Signature : size to be defined
Algorithm : To be specified

10.3.6.2.7 Signature generation algorithm (Sig_u)

Who : User
Purpose : To sign data sent to the Network Operator
When : Whenever a signature must be sent to the Network Operator
Input : Output data of h3 : size to be defined
User secret key : size to be defined
Output : Signature : size to be defined
Algorithm : To be specified

10.3.6.2.8 Signature verification algorithm

Who : Network operator
Purpose : Verify user generated signatures
When : Whenever a signature is sent from user to Network Operator
Input : Signature : size to be defined
User public key : size to be defined
Output data of h3 : size to be defined
Output : TRUE if signature ok, FALSE otherwise
Algorithm : To be specified. It must correspond to the signature generation algorithm

10.3.6.2.9 User Certificate Verification algorithm

Who : Network operator
Purpose : Verify user certificate and retrieve public key from it
When : When a certificate is sent from user to Network Operator
Input : Certificate : size to be defined
Certification Authority public key : size to be defined
Output : TRUE if certificate ok, FALSE otherwise
Additional output if certificate is ok :
User's public key : size to be defined
Algorithm : To be specified

10.3.6.2.10 Network Operator Certificate Verification algorithm

Who : user
Purpose : Verify Network Operator certificate and retrieve public key agreement key from it
When : When a certificate is sent from Network Operator to user
Input : Certificate Network operator : size to be defined
Certification Authority public key : size to be defined
Output : TRUE if certificate ok, FALSE otherwise
Additional output if certificate is ok :
Network Operator's public key agreement key : size to be defined
Algorithm : To be specified

11. References

[1] ETSI Technical Report, "Scenarios and Considerations for the Introduction of the Universal Mobile Telecommunications System (UMTS)", DTR/SMG-050104, v.1.0.0, 1 April 1996.
[2] UMTS Task Force Report, "The road to UMTS", Brussels, 1st March 1996
[3] Samukic Antun, Polese Pietro, "Migration/evolution towards UMTS - Market Driven Approach in Research and Standardization", RACE Mobile Telecommunications Summit 1995, Cascais, 22-24 November 1995.
[4] Radio Equipment and Systems, DECT System Description Document, ETSI, Draft v.3.4., June 1992
[5] GSM 02.09, Security aspects, version 4.2.4
[6] ACTS AC095, Initial report on security requirements, AC095/ATEA/W21/DS/P/02/B
[7] GSM 04.08, Mobile radio interface layer 3 specification, version 4.9.0
[8] GSM 11.11, Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, version 4.13.1
[9] GSM 09.02, Mobile Application Part (MAP) specification, version 4.12.0
[10] GSM 03.03, Numbering , addressing and identification, version 4.9.0
[11] GSM 03.20, Security related network functions, version 4.3.1
[12] ACTS AC095, Security services : First Specification, AC095/RHUL/W23/DS/P/07/A.1