Project Number	AC095
Project Title	ASPeCT: Advanced Security for Personal Communications Technologies
Deliverable Type	Intermediate
Security Class	Public

Deliverable Number	D17
Title of Deliverable	**Migration scenarios: final version**
Nature of the Deliverable	Report
Document reference	AC095/ATEA/W21/DS/P/17/1
Contributing WPs	WP2.1
Contractual Date of Delivery	August 1997 (Y03M06)
Actual Date of Delivery	16 October 1997
Editors	Geneviève Vanneste, Bart Franco

Abstract	In this deliverable the applicability of the authentication framework as a basis for a migration scenario has been evaluated. The features offered by the authentication framework, are evaluated on compliance with the UMTS requirements. Packet based services are studied. The Authentication Framework is then discussed in the context of a generalised Packet based network. A possibility is given how to integrate the UMTS framework within the UMTS architecture. During evaluation topics for further elaboration have been identified: • changed security requirements by the introduction of services • security for packet based services • mapping of the security framework and mechanisms on the UMTS architecture • integration of the authentication framework into the UMTS signalling
Keywords	ACTS, ASPeCT, UMTS, security, architecture, packet based,

	migration

1.Executive Summary

In this deliverable the applicability of the authentication framework as a basis for a migration scenario has been evaluated.
The UMTS services are summarised and a classification scheme is described. The security requirements for UMTS are summarised, together with the security features and a classification of security mechanisms. The features offered by the authentication framework, are evaluated on compliance with the UMTS requirements.
Packet based services are studied. Packet based networks are introduced and the difference between a Packet based network and circuit switched network is explored. Four generic types of Packet based networks are presented. The Authentication Framework is then discussed in the context of a generalised Packet based network.
An overview is given of the current available ideas on the UMTS role models and the physical and logical model for the UMTS architecture. A possibility is given how to integrate the UMTS framework within the UMTS architecture.
As a result of the above, evaluation topics for further elaboration have been identified:

- changed security requirements by the introduction of services
- security for packet based services
- mapping of the security framework and mechanisms on the UMTS architecture
- integration of the authentication framework into the UMTS signalling

Table of Contents

2.Introduction

In this deliverable the applicability of the authentication framework is checked within different contexts.

In section 5 the UMTS services are summarised and a classification scheme is described. The security requirements for UMTS are summarised, together with the security features and a classification of security mechanisms. The features offered by the authentication framework, are evaluated on compliance with the UMTS requirements.

In section 6 packet based services are studied. Packet based networks are introduced and the difference between a Packet based network and circuit switched network is explored. Four generic types of Packet based networks are presented. The Authentication Framework will then be discussed in the context of a generalised Packet based network.

In section 7 an overview is given of the current available ideas on the UMTS role models and the physical and logical model for the UMTS architecture. A possibility is given how to integrate the UMTS framework within the UMTS architecture.

2.1.Contributors

This is a list of all project managers involved in the ASPeCT project plus the principal editor (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 6407267 Fax: +30 1 6407039	vithynos@panafon.gr
John Shaw-Tayler	Royal Holloway, University of London Egham Surrey TW20 0EX England	Phone: +44 1784 443430 Fax: +44 1784439786	jst@dcs.rhbnc.ac.uk
Günther Horn	Siemens AG ZFE T SN 3 D-81730 München Germany	Phone: +49 89 636 41494 Fax: +49 89 636 48000	Gunther.Horn@mchp.siemens.de
Geneviève Vanneste	Siemens Atea Atealaan 34 B-2200 Herentals Belgium	Phone: +32 14 252937 Fax: +32 14 253339	p82586@vnet.atea.be
Eric Johnson	GIESECKE & DEVRIENT GMBH	Phone: +49 89 4119 944	X400: c=de; a=cwmail; p=g+d; s=johnson; g=eric

	Prinzregenstr. 159	Fax:	+49 89 4119 905	
	D-81607 München			Internet:
	Germany			100277.1206@compuserve.com
Nigel Jefferies	Vodafone Ltd	Phone:	+44 1635 503883	Nigel.Jefferies@
	The Courtyard			vf.vodafone.co.uk
	2-4 London Road	Fax:	+44 1635 31127	
	Newbury			
	Berks RG14 1JX			
	England			

2.2.Document History

Revision	Date	Changes
1	16/10/97	first version

3.References

[1] UMTS 01.04, “Special Mobile Group (SMG); Scenarios and considerations for the introduction of the Universal Mobile Telecommunications System (UMTS)”, May 1996.

[2] RACE 2066 Mobile Networks (MoNet) project, CEC Deliverable No R2066/BT/PM2/PS/P/070/b2, "*UMTS system structure document*", Issue 2.0, Dec. 1994.

[3] UMTS 22.01, “Universal Mobile Telecommunications System (UMTS); Service aspects; Service principles”, July 1997.

[4] UMTS Task Force Report, “The road to UMTS”, March 1996.

[5] GSM 02.09, “European digital cellular telecommunications system (Phase 2); Security aspects”, September 1994.

[6] ETR 330, “Security Techniques Advisory Group (STAG); A guide to the legislative and regulatory environment”, November 1996.

[7] PAC EG5 Report, “Global Multimedia Mobility (GMM); A Standardization Framework for Multimedia Mobility in the Information Society”, October 1996.

[8] UMTS 09.01, “Special Mobile Group (SMG); Security principles for the Universal Mobile Telecommunications System (UMTS)”, June 1996.

[9] AC095/ATEA/W21/DS/P/05/A, Migration Scenarios, ACTS ASPeCT deliverable, August 1996.

[10] UMTS Forum, A regulatory framework for UMTS ; version 2.3.0

[11] ETS UMTS 23.01, General UMTS Architecture, version 0.0.7

4.Abbreviations

AC	Authentication Centre
ACTS	Advanced Communications Technologies and Services
AMV	the Agnew-Mullin-Vanstone equation
AN	Access network
ASPeCT	Advanced Security for Personal Communications Technologies
Au/Gbu	Reference point between IWU1 and GSM/UMTS
Bu	Reference point between IWU3 and B-ISDN/UMTS
CA	Certification Authority
CN	Core Network
CP	Content Provider
CS	circuit switched
Cu	Reference point between USIM and ME
ETR	ETSI technical report
ETSI	European Telecommunications Standards Institute
FSM	Finite State Machine
GSM	Global System for Mobile communications
HN	Home network
Iu	Reference point between AN and IWU
IWU	Interworking unit
MS	Mobile station
NO	Network Operator
Nu	Reference point between IWU2 and N-ISDN/UMTS
PB	Packet Based
Pu	Reference point between IWU4 and PDN/UMTS
SIM	Subscriber Identification Module
SIM	Subscriber identification module
SN	Serving network
SP	Service Provider
UIM	User Identity Module
UMTS	Universal Mobile Telecommunication System
USIM	UMTS SIM
Uu	UMTS radio interface
VASP	Value added service provider

5. UMTS Services

5.1. UMTS Services

5.1.1. General

Future mobile telecommunication systems will offer a wide range of telecommunication services to mobile users. This document provides an overall description of these services and of their main features. In this document we address the following aspects. First, we present the framework that describes UMTS service provisioning. Second, we present the UMTS services, via a general UMTS service classification scheme. Third, we present existing (or specified) capabilities for controlling the services.

5.1.2. Service provision framework

UMTS will offer a wide range of high quality services to mobile users. Since UMTS is envisaged as the mobile extension of B-ISDN, its services should be compatible with those provided by B-ISDN, ISDN, PSTN and pre-UMTS technologies (e.g., GSM, DCS 1800 etc.). Hence, the aim, apart from supporting traditional mobile telephony, is to support also multimedia services (of course under the limitations imposed by the radio path, that constitutes the interface among the mobile users and UMTS) [1].

Following advanced service provisioning methodologies, UMTS services are composed in a modular way by combining independent service components [2] (see Figure 1). Service components may be seen as reusable pieces of software, providing functionality such as *service control*. Service control may be seen as the functionality necessary for accessing, releasing, using and modifying a service.

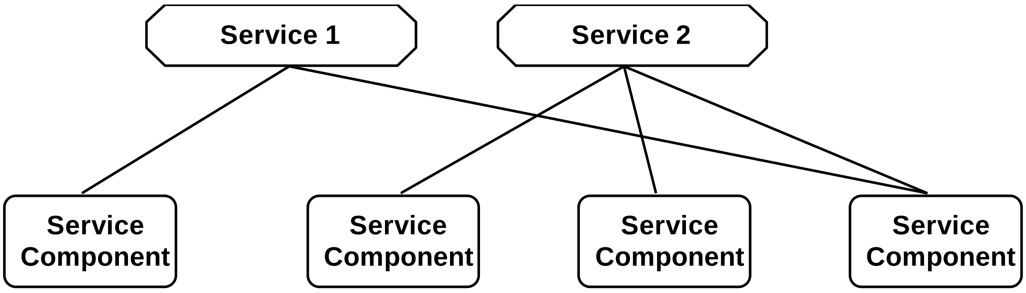

Figure 1: UMTS services construction

UMTS aims at supporting the widest possible variety of services, and of providing the UMTS users with the broadest possible range of service control capabilities. Figure 2 illustrates the basic UMTS service provision framework, which supports these aspects [3]. A basic aspect is the separation among bearer control, call control, and mobility management. Bearer control enables the information transfer of an information flow. For example, incorporated in this context is the functionality for adding/removing information flows. The ability of requesting different types of bearers is assumed, in order to support the requirements of the various information flows. Call control is more related to the users involved in the call, in the sense that it provides functionality for adding or removing users from a call, for performing user profile inspections, etc. Finally, mobility management enables service provisioning to mobile users (i.e., location monitoring, location updating, handover control, etc.). The role of the service platform is to provide the interfaces among the service provider and the mobile network operator, especially in case the service provider and the network operator are completely independent entities.

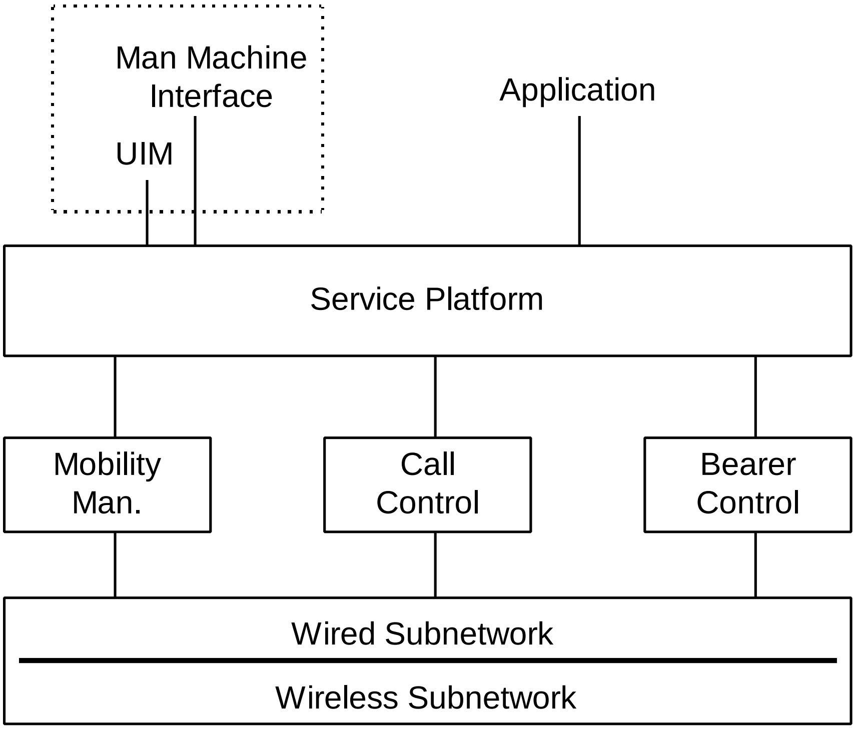

Figure 2: Service provision framework

5.1.3. Services classification scheme

UMTS services may follow a general classification scheme (i.e., a scheme that is valid for other communication systems as well). In this perspective, UMTS services may be seen as the combination of a *service type* (i.e., conversation, conference, retrieve, distribution, messaging) and of one or more *information flows* (i.e., audio, video, data etc.). In the rest of this section we briefly explain these aspects.

5.1.3.1. Service types

The UMTS service types may fall in one of the categories below.

A. Interactive services, subdivided into:

- *Conversational services*. They involve a connection-based, point-to-point, and bi-directional communication. Their requirements are low delay and delay variation. They are error and loss tolerant to a certain extent. The classical example of such a service is telephony.

- *Conferencing services*. They involve a connection-based, point-to-multipoint communication. They may be seen as a generalization of the conversational services, since the difference is that conferencing services involve many users. Similarly, as the conversational services, they require low delay and delay variation, and are error and loss tolerant to a certain extent. A classical example is the video-conference service.

- *Retrieval services*. Their characteristics are that they involve connection-based, point-to-point or multipoint-to-point, and unidirectional communication. Such services enable users to retrieve different kinds of information from particular information sources, databases. The direction of the communication is from the sources to the users. The requirements are low delay, and error and loss free communication.

- *Messaging services*. They involve connectionless, point-to-point or point-to-multipoint, and unidirectional communication. They enable the forwarding of information units in a non real time manner. They may be seen as a generalization of the e-mail service. No delay or delay variation constraints exist. A requirement is error and loss free communication.

B. Distribution services, subdivided into:

- *Distribution services without user control*, where information is provided by a central source, without enabling the user to have control of the information flow administration, e.g. television or audio broadcast services

- *Distribution services with user control*, where user is enabled to access broadband information distributed in separated information cells and to control the start and the order of the presentation of the information

A general comment deduced from the classification above is that it is based on the following aspects. First, the manner of the communication, and especially on whether it is *connection based* or *connectionless*. Second, on the *point-to-point* or *point-to-multipoint* distinction. Third, on the direction of the communication, i.e., on whether it is *unidirectional* or *bi-directional*. Regarding the communication manner distinction (which is the most important one) we can make the following comments. Connection oriented communication services are suitable for real-time communication (i.e., for communications where there are delay constraints). Connectionless services involve information transfer from one user to one or more users in an asynchronous way. The main differences between the connection oriented and the connectionless communication manner are the following. In the former, there is a connection establishment phase prior to the information transfer phase, while in the latter there is only an information transfer phase. Connectionless communication services do not require recipient availability, while this is not feasible in connection-mode communication services.

5.1.3.2. Information flow

The service types may involve the transfer of audio, video, data, text, graphics, and pictures [4]. Aspects that determine the requirements of the information flows are the following. First, their categorization as rate-oriented (audio and video) or unit-oriented (data, text, graphics, pictures). Second, their inherent characteristics (e.g. integrity is more essential for data transfer than for audio transfer), and the required Quality of Service (QoS) levels.

5.1.4. Service control capabilities

UMTS users should be provided with advanced service control capabilities. A list of pertinent capabilities may be (but is not restricted to) the following.

- Session management, which allows the user to prepare the system for the service provision

- Set-up, which allows a service user to set up the connections (in other words to reserve the resources) required by the communication

- Release, which allows a service user to release the connections (in other words to reserve the resources) required by the communication

- Allocate, which allows a service-user to allocate resources in an existing connection oriented communication in which this user is involved

- De-allocate, which allows a service-user to de-allocate resources, that were used in a connection oriented communication
- Modify, which allows the service-user to modify some features of the communication
- Negotiate, which allows both the service-user and the system to negotiate the characteristics of a communication (e.g., QoS levels)
- Authenticate, which allows a service-user and the system to authenticate each other
- Charge, which enables the user to be informed about charging schemes. Charging information may be presented any time. In the special case of incontestable charging this kind of information must be signed by the user and returned to the system
- Interrogate, which allows the service-user to obtain service management information
- Select, which gives the user the opportunity to select among a list of possible conditions
- Report, which allows the system to indicate exceptional conditions

5.2.Security requirements for UMTS services

5.2.1.Security features of contemporary mobile systems

In second generation mobile systems, the communication between the parties involved should be protected against third party intrusion, as eavesdropping, modification of the transferred data or impersonation of subscribers or networks by unauthorised parties. Protection of the users privacy rights is also an important security requirement. Thus, the corresponding security features that contemporary PLMNs should possess are [5]:

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

In the second generation mobile systems, a security feature is either a supplementary service to bearer or teleservices, that can be selected by the subscriber, or a network function involved in the provision of one or several telecommunication services.

5.2.2.Security requirements for UMTS

The security requirements of the third generation mobile services are evolving. The use of telecommunications has grown in importance in all financial and social sectors to the point where many organisations are totally dependent upon their networks. New environments are emerging, providing users with increased mobility. Furthermore, there is a trend for services to be supplied by more than one network operator, resulting from the gradual liberalisation of the telecommunications market. Therefore, telecommunications security requirements are changing for four main reasons [6]:

- liberalisation of telecommunications (infrastructures, services and terminal equipment)
- evolution in technology and services
- increasing dependence upon, and expectations from telecommunications services by the users, especially regarding the quality of service
- furthering of national and international requirements with regard to legal interception of telecommunications, for purposes of national security and the fighting of organised crime

The security of telecommunications is therefore affected by many factors, including technical, operational, social and legal. It encompasses the particular requirements for all parties involved, namely users, network operators and service providers.

Considering the contemporary increased security requirements as well as the general features of UMTS, it is obvious that the objectives of security in UMTS will be a superset of the security objectives of the second generation systems. Some additional requirements are as follows [7]:

- the UMTS security features must be compatible with the world-wide availability of UMTS
- the security features provided by UMTS must be adequately standardised to enable secure world-wide interoperability and roaming between different network operators
- the level of protection afforded to users and providers of UMTS services must be at least equal to that provided in contemporary fixed networks
- the security policy of UMTS operators must incorporate fraud management
- the lawful interception of a user’s communications must be feasible
- the emergency services must be adequately protected against abuse

The different types of information that will be available will usually require also different kinds of protection. Therefore, the security requirements must reflect the features of the various types of information that can arise in UMTS. These types can be defined as follows:

- **user traffic**: all information transmitted on the end-to-end traffic channel between users.
- **charging, billing and accounting**: information relating to charges incurred either by users whilst using network resources and services (NOs to SPs), or by subscribers for their subscriptions and user's charges (SPs to subscribers).
- **location**: location information regarding a user or terminal equipment
- **dialling**: information relating to diallable numbers associated with users
- **routing**: information passed through the network to enable correct routing of calls, using location and dialling information
- **identity**: information which determines the identity of an entity (users, subscribers, terminal equipment)
- **security**: information relating to security and access control, including encryption keys, authentication messages, PINs and databases of identities generated by service providers and network operators

5.2.3.Security features for UMTS

The different security features for UMTS can be assigned to the following categories and subcategories [8]:

I. **authentication**

A. entity authentication: mutual verification of identity between entities

B. transmitted data origin authentication: verification of identity of the data originator by the data receiver

II. **confidentiality**

assurance that data are not made available or disclosed to unauthorised parties

III. **anonymity**

assurance that an entity cannot be identified by unauthorised parties

IV. **access control**

A. access control to equipment: assurance that entities can only use equipment for which they are authorised

B. access control to a service: assurance that entities can only use services for which they are authorised

C. access control to data: assurance that entities can only access data for which they are authorised

V. **integrity**

protection of data against manipulation by unauthorised parties

VI. **non-repudiation**

A. non-repudiation of origin of transmitted data: verification that a transmitted message originated from a specified entity
B. non-repudiation of delivery of transmitted data: verification that a transmitted message was received by a specified entity
C. non-repudiation of access to data: verification that a specified entity gained access to data
D. non-repudiation of access to services: verification that a specified entity gained access to services
E. non-repudiation of procedure involvement: verification that a specified entity was involved in a certain procedure

VII. supplementary

assurance that the service provider or network operator can provide end-to-end security services to particular fixed or mobile users, subject to the availability of additional end user equipment

5.2.4.UMTS security mechanisms

The following requirements for UMTS security mechanisms are being identified by ETSI [8]:

1) Use of the minimum of long-distance real-time signalling. For instance, the need for international signalling connections at every location update or call when roaming should be avoided.
2) Use of the minimum of bilateral pre-arrangements between service providers and network operators.
3) Possession of the means to manage cryptographic keys which may need to be exchanged by service providers and network operators.
4) Ease of distributing and changing cryptographic keys by the users of the security mechanisms.
5) Standardisation only to the extent needed for interoperability and roaming.
6) Support of version control management to allow for subsequent upgrading and revision of mechanisms.
7) Possession of the means to detect and report security violations as well as the means to restore the system to a secure state.
8) Compliance with legal requirements imposed by national authorities, including export controls and lawful interception.

Naturally, there exist various approaches for realising a particular (type of) mechanism. Some of the approaches are described below, classified by security category:

I. authentication

A. symmetric
B. public key
C. cryptographic check functions
D. zero knowledge

II. confidentiality

A. block ciphers (symmetric, asymmetric)
B. stream ciphers

III. anonymity

A. identity confidentiality (symmetric, asymmetric)
B. temporary identities
C. anonymous access

IV. access control

A. non-cryptographic authentication (personal identification numbers, simple challenge - response, biometrics)
B. registration
C. type approval
D. barring
E. auditing
F. physical means

V. **integrity**
   A. non-cryptographic integrity (error detection / correction, CRCs);
   B. cryptographic check functions
   C. MACs
   D. hash functions

VI. **non-repudiation**
   A. symmetric
   B. asymmetric

5.3.Applicability of the authentication framework

The service provision is separate from the authentication and must follow it. Some of the necessary exchanges in the service provision procedure could occur within the authentication framework procedures. Nevertheless, the subsystems modularity (e.g. security, mobility, service provision, etc.) is a key objective in UMTS, in order to ensure 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. The authentication may not be performed only in a number of special services, for example in emergency calls without a subscriber card.

5.3.1.UMTS requirements on the authentication framework

The UMTS primary goal for flexibility and global interworking leads to the necessity for support of multiple authentication mechanisms by the communication carriers. It is even foreseen that the set-up of roaming agreements between operators and service providers may be dynamic. Thus, a common description format for authentication mechanisms is essential, which will result in a set of requirements to the signalling procedures.

Regarding the implementation of authentication mechanisms in UMTS, the trade-off between flexibility and efficiency should be considered. It is likely that the message exchange and signalling required will increase with enhanced flexibility, as regards the support of different authentication mechanisms. In view of this, the information flows and message fields required to support authentication should be specified as far as possible, while retaining the necessary flexibility for UMTS. Thus, a framework should comply with a series of requirements:

1) support of both public key and symmetric key approaches
2) support of existing mechanisms (e.g. GSM, DECT, UPT)
3) ability for mechanisms to be upgraded in the future
4) planning for different mechanisms to be used by different service providers
5) definition of the procedure of obtaining and distributing information on the authentication capabilities (e.g. algorithms, parameters, certificates, etc.) of all parties involved
6) definition of the generic information flows and message fields, in order to support the modular approach for UMTS
7) definition of the interaction between the mobility procedures and the authentication procedures, especially the common parameters or requirements on the interfaces

5.3.2.Features of the authentication framework

The authentication framework, as proposed by ASPeCT [9], aims to provide a flexible procedure for user-network authentication by allowing a number of different mechanisms and algorithms to be incorporated, with the ability to migrate smoothly from one mechanism to another.

This framework allows the authentication capabilities of users, network operators and service providers to be taken into consideration for the selection of the mechanism to be used. A list of capability classes, including the mechanisms supported, will need to be maintained so that different entities (users, network operators, service providers and trusted third parties) can negotiate these mechanisms.

5.4.Conclusion

Examining the features of the authentication framework, it can be observed that it is compliant with the majority of the UMTS requirements, listed in the previous section. Both public key and symmetric key approaches are supported, permitting different service providers to use different mechanisms. The procedure for distribution of the authentication capabilities information and the information flows are clearly defined, thus supporting the UMTS modular approach. The user anonymity is preserved throughout the authentication process.

Finally, the cost of additional information transfer is minimal, compared to the extensive flexibility in selecting the authentication mechanism which will be imperative for a UMTS environment.

6.Packet Based Services

6.1.Introduction

Part of the purpose of the Deliverable D17 is to study the existing proposed Authentication Framework, and to suggest enhancements that may be required to reflect current developments in UMTS. The probable use of packet based services within UMTS may require modification to the existing proposed authentication framework. In particular, it is necessary to ensure that the Authentication Framework will meet the security requirements of a packet based network.

For this reason, this section will look at Packet Based (PB) networks, and explore any extra requirements that these impose on the Authentication Framework. It will begin with an introduction to PB networks, and explore the difference between a PB network and a Circuit Switched network. After this, the four generic types of PB networks will be presented. The Authentication Framework will then be discussed in the context of a generalized PB network, and finally there is a conclusion for the section.

6.1.1.Packet based services

A Packet Based service uses a fundamentally different mechanism for information transfer than does a Circuit Switched service.

In a Circuit Switched (CS) service, the Calling Station uses a Call Request signal to establish a single route between itself and the Destination Station. Once received by the Destination Station, a Call Accept signal is returned along the created path. Once this is received by the Calling Station, the information transfer can begin. While the call is supported, the Network resources used en-route between the Calling and Destination Stations are dedicated to this call. This results in a high utilization for voice connections. However, for data connections, much of the time the line is idle. A further limitation on the Network is that the transmission rate must be the same as the receive rate at the other end. Both of these problems are addressed by a Packet Based Network.

A Packet Based (PB) Network views the Network in a fundamentally different way. The PB Network is considered to be composed of an array of nodes, where each node can communicate with a set of surrounding nodes. Data within the Network is divided up into and transmitted as short packets. Each packet is composed of the User's data, and sufficient control data to allow the Network to route the data to its destination. This is achieved by a packet at a node in the Network determining which is the best node to be forwarded to according to some criteria. Examples of criteria are queue size at the destination node, quality of link, speed of link etc. The packet is then forwarded to the chosen node once the link is available. This approach has several advantages.

- The link is dedicated only whilst sending the packet, thereby making it available for other messages at other times.
- When traffic becomes heavy on the Network, less busy nodes can be utilized, thereby reducing the congestion.
- Stations can exchange data at different data rates, since each connects to its node at the proper data-rate.
- Priorities can be used to give certain types of information higher priorities through the Network.

6.1.2.Different Approaches to Packet Based Operation

For a Packet Based Network, there are two distinct internal views and two distinct external views. Internally, the PB Network may operate in either a virtual circuit or datagram mode.

A virtual circuit PB Network appears quite similar to a Circuit Switched Network. A Call Request packet is sent through initially that is analogous to the Call Request signal in CS Networks. Once a Call Accept packet is received, then that path is used for all subsequent packets of the message. However, each packet is still queued at each node, and so transfer is therefore slower than the Circuit Switched Network.

A data gram PB Network does not require call set-up. It is therefore faster for short calls than the virtual circuit PB and potentially the Circuit Switched Network. The path of each packet is assessed at each node, and the packets forwarded once the link becomes available. For large volumes of data, this extra processing for every packet at each node may mean that the virtual circuit approach is superior.

In addition to these two internal modes of operation, there are the following two external views which can be combined with the above to produce four separate modes of operation.

The two external modes are either connection-orientated or connectionless service.

The connection-orientated service treats the data as it enters the Network as a sequenced order of data packets, and guarantees delivery to the destination station in the same order. This is also called an *External Virtual Circuit* service.

The connectionless service just takes all data in as individual packets, and delivers them when they arrive at the destination station with no guarantee of ordering. This is also called an *External Datagram* service.

This means that there are four different Networks that can be defined:

- External Virtual Circuit + Internal Virtual Circuit - Packets that go in, are all transmitted along the same path, and come out in the same order.
- External Virtual Circuit + Internal Datagram - Packets enter the Network in a defined order, are then forwarded through the Network to the destination, and are then buffered until such a time as they can be delivered in the correct order.
- External Datagram + Internal Datagram - Packets enter the Network in a defined order, but are then individually forwarded throughout the Network and delivered to the destination in the order that they arrive at the final node.
- External Datagram + Internal Virtual Circuit - Packets are sent in a defined order, are transmitted along a single defined path, but are not guaranteed to be in order. This makes little sense as the packets will be ordered within the Network, but not guaranteed to be in order when delivered.

6.2.Use of proposed ASPeCT authentication mechanisms within a Packet Based Network

The ASPeCT Authentication Framework and Security Migration scheme has to be considered against the context of the above mechanisms of PB operation.

For UMTS, the full requirements for security are defined in ‘Security principles for the Universal Mobile Telecommunications System (UMTS 09.01)’ [8]. A number of requirements are given here as examples of the kind of security specified.

There are requirements that an intruder shall be prevented from masquerading as a valid User, SP or NO, that both User and Network traffic needs to be secured against interference, and that privacy of such traffic can be ensured. In addition, Network entities need to be authenticated to one another, whilst the integrity of messages passed between entities needs to be ensured, as does confidentiality and anonymity for the User. Against this, the mechanisms need to be efficient in terms of the number and size of the message, with adequate performance of the chosen implementation.

In addition to the above, there may be a requirement that a Network disables the encryption of User traffic, whilst still requiring that its signalling and management information is secure. (Here User traffic means any traffic that is generated by the User.) Within GSM, if the User data is un-encrypted, then all Network data is un-encrypted, which opens up the Network for attack. Clearly this is unacceptable within UMTS, so an additional requirement can be stated which is that the protection of User and Network data must be considered as independent requirements.

Hence, there are two types of information transfer that need to be discussed, User data and Network data. The difference is expanded upon below.

The User data is logically distinct from the Network data. It consists of the User generated data which is embedded within packets for distribution through the Network.

The Network data consists of both the routing and authentication information which surrounds the User data within the packets, and non-User Network information such as signalling and management data contained within the packets. This definition is given to help clarify the requirement that it should be possible to protect the User and Network independently.

The existing discussion of the Authentication framework [9] is concerned with authenticating the physical User to the Network, and not authenticating the Mobile Station (MS) to be part of the Network. Within a PB Network, the MS may become a node within the Network, and hence there is a complete set of requirements for the authentication and registering of the MS which are currently missing. It is logically important to draw a distinction between User and MS authentication, as they satisfy very different requirements.

6.2.1.Requirements for security in User data

The Authentication Framework currently authenticates the User, and establishes the encryption key to be used for data traffic. The messages required to establish this key and authenticate the User are distributed as Network traffic, and are carried as data within packets. These cannot be encrypted between the User and the NO as no key has been established at that point. However, the information that is distributed does not allow the Network entities to be compromised.

Once this key is established, then any User data such as voice traffic can be encrypted using this key. These messages are sent as User data within the packets, and are surrounded by the Network data related to routing and authentication.

This satisfies the requirements for establishing an encryption key, and for providing security for the User data. However, there are no requirements addressed with regard to the Network data.

6.2.2.Requirements for security in Network data

A discussion of the mechanism used to secure the Network data will be independent of the Packet Based approach used. All PB approaches use a similar technique of taking the data and surrounding it with the routing information that the Network requires. For example, in ATM, the 53 octets are composed of 48 octets of data prefixed with 5 octets of routing information. The type of PB Network used will not be defined, rather a generalised discussion will be used.

6.3.Overall requirements for security

A discussion on security in PB networks can be based on a generalised network, rather than a dedicated discussion for each type of network. This discussion will be expanded in this section to look at both end-to-end authentication and node to node authentication.

6.3.1.General assumptions

The Authentication Framework provides a mechanism whereby a secret key can be established between the User/MS and the NO. In addition, this framework ensures that the key cannot be discovered by a third party. Hence this mechanism can be used as the basis of both User authentication and node authentication. At the moment the key is only used for User authentication. However, this key on its own is insufficient to stop a third party capturing the message and re-sending it, as it would still appear to be a valid message as far as all parties are concerned. This is called a replay attack. To get around this, a parameter which changes in time is also required to vary the encryption for each message, and this must be done in such a way as to allow the receiving end to also obtain this parameter for authentication. Examples of such a parameter may be time-of-day, frame number etc.

6.3.2.End-to-end authentication

The above key can be used to encrypt any data that is to be passed end to end. As the key is only known by the User and the NO, then any data that is sent between the two cannot be decrypted by an unauthorised party. If this data is encrypted, then a correct decryption at one end is sufficient to ensure that the message came from the other.

This works in a similar way to a Message Authentication Code (MAC), but instead of using the key to encrypt a part of the message and append this to the message, the entire message itself is encrypted. However, it may be necessary for reasons of information security to use an appended MAC to authenticate the message.

6.3.3.Node-to-node packet authentication

In addition to the above authentication, the source and validity of a packet needs to be authenticated when received by the next node. As a prerequisite of this, the nodes need to authenticate each other. To achieve this authentication in practice may require some kind of signature to be appended to the packet. This signature can be generated in a number of ways, two valid approaches being a certifiable public key and a shared secret key. However, there is clearly a large processing requirement associated with digital signatures. Hence, if a less processor intensive method could be found, then it would clearly be advantageous.

6.4.Conclusion

Clearly there is a large area of network authentication that has yet to be explored. The Authentication Framework works well as a way of establishing the keys to be used in encrypting User data. However, before the Authentication Framework can be accepted fully, it needs to be demonstrated as compatible with the network authentication mechanism used.

7.UMTS network

In this section an overview is given of the current available ideas on the UMTS role model and the physical and logical model for the UMTS architecture.
In a second part one possibility is given how to integrate the UMTS framework within the UMTS architecture.

7.1.UMTS role model and architecture

Different role models can be found in literature.
The UMTS forum defined the UMTS market players [10]

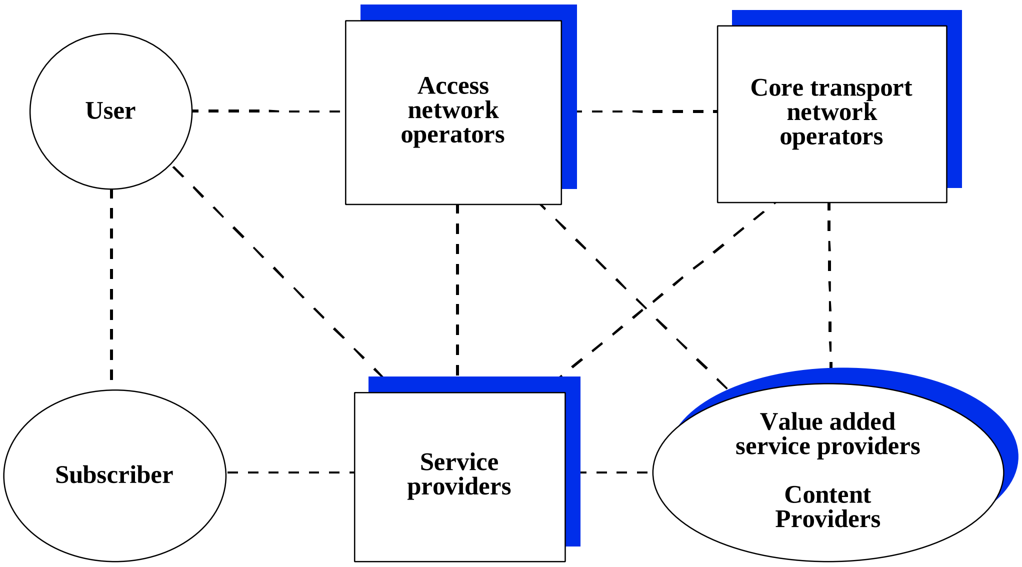

Figure 1 UMTS Forum - UMTS market players

Two other role models are defined in the draft ETS on “service aspects: service principles” [3] and in the draft ETS on “General UMTS architecture” [11], described hereafter:

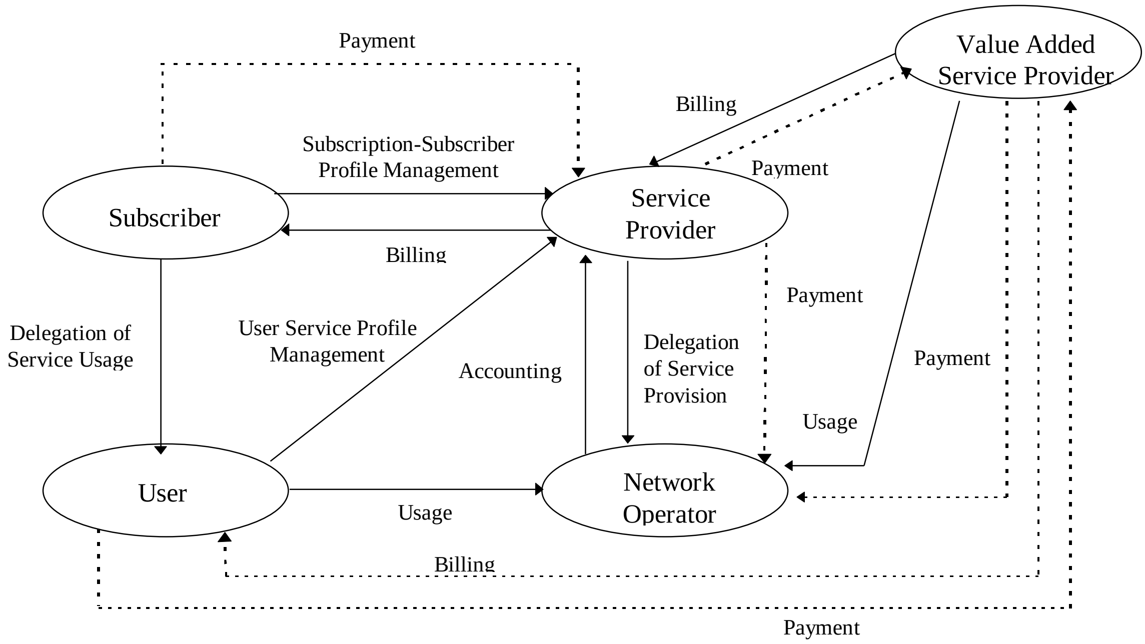
Payment
Value Added Service Provider
Billing
Subscription-Subscriber Profile Management
Payment
Subscriber
Service Provider
Billing
Payment
Delegation of Service Usage
User Service Profile Management
Accounting
Delegation of Service Provision
Payment
Usage
User
Usage
Network Operator
Billing
Payment

Figure 2 ETS 22.01 - UMTS role model

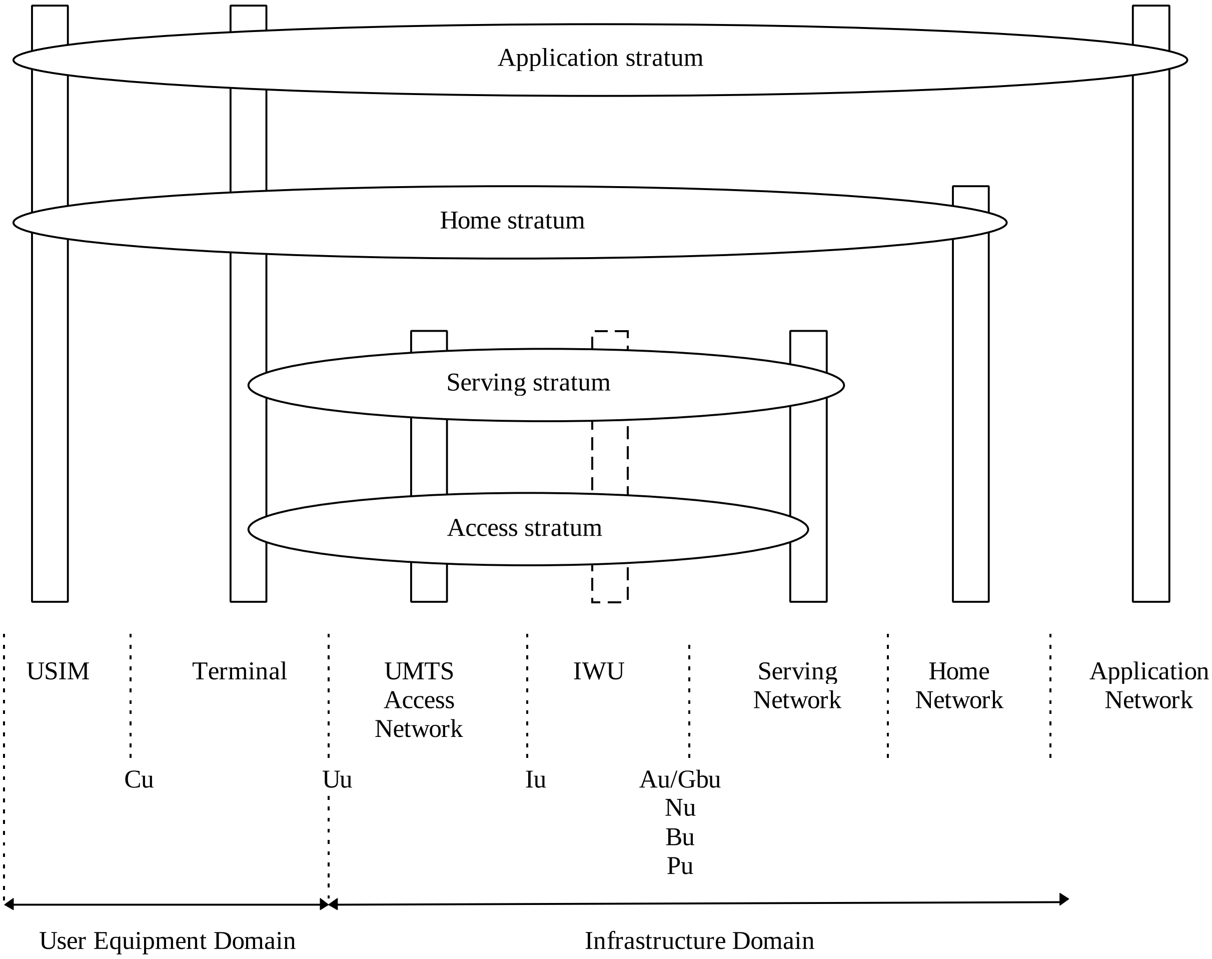

Figure 3 ETS 23.01 - UMTS domains and strata

In the UMTS Forum market model, the Network operator role is split up into an Access Operator and a Core network operator.

The role model used in [11] is not completely aligned with the one defined in [3]. Following conversions can be done:

23.01	22.01
IWU[1] + Serving Network	Core Network
Home Network	Service Provider
Application Network	Value added Service Provider / Content provider
CN = SN + HN	

In the remaining sections the role model defined in ETS 23.01 will be used. Therefore it is elaborated hereafter.

The physical aspects are modelled using the domain concept. A domain is defined as a high level groupings focusing on physical entity aspects, and comprising all the functionality in those entities. A module is then seen as a specific instance of a domain with the capability to provide a subset of the functions of one or more strata.
A basic architectural split is between the user equipment (terminals) and the infrastructure, this results in two domains: the User equipment domain and the Infrastructure domain.
The user equipment domain itself can again be split up into several elements. One example is the USIM, a removable smartcard. The levels of functionality from the user equipments can vary, e.g. dual mode UMTS-GSM terminals.
The Infrastructure domain is further split into the Access Domain, characterised by being in direct contact with the User Equipment and the Core Network Domain. The Access Domain comprises roughly the functions specific to the access technique, while the functions in the Core network domain may potentially be used with information flows using any access technique. This split allows for different approaches for the core network domain, each approach specifying distinct types of Core Networks connectable to the Access Domain, as well as different access techniques, each type of Access Network connectable to the Core Network Domain.
The Core network is further split into the Serving Network and the Home Network. No more work is available on how the tasks will be assigned.
The Application Network Domain is defined but not further described. This can be seen as the equivalent to the VASP, value added service provider, or CP, content provider, described in the UMTS role models.

The logical aspects are modelled using the strata (plural of stratum) concept. The stratum is defined as a high level functional groupings focusing on one or more protocols, and comprising all the entities involved in those protocol.
The Access stratum is the functional groupings consisting of the parts in the infrastructure and in the user equipment and the protocols between these parts being specific to the access technique (i.e. the way the specific physical media between the User Equipment and the Infrastructure is used to carry information). Functions related to control and management of the radio resources are located in this stratum.
The Serving stratum consists of protocols and functions to route and transmit data/information, user or network generated, from source to destination. The source and destination may be within the same or different networks. Functions related to telecommunication services and mobility management may be located in this stratum.
The Home stratum contains the protocols and functions related to the handling and storage of subscription data and possibly home network specific services. Functions related to subscription data

[1] The IWU is sometimes mentioned explicitly next to the core network.

management, customer care, mobility management, including billing and charging, may be located in this stratum.
The Application stratum includes end-to-end protocols and functions which make use of services provided by the home, serving and access strata and infrastructure to support value added services. End-to-end functions are applications which are consumed by users at the edge of/outside the overall network. The applications may be accessed by authenticated users who are authorised to access such applications. The users may access the applications by using any of the variety of available user equipment.

7.2.Authentication framework in the UMTS architecture

Once a connection-oriented signalling channel (or part of a channel) between the user and the network is set up, the security procedures have to take place, before any real services are given to the user.
The Serving network has no role to play within the security procedures. (CN = SN + HN). The procedures run between the user (smart card) and the HN (or the AN on behalf of the HN).

It is not clear how these procedures fit into the strata model, they seem to belong to the home stratum.

The messages defined in the authentication framework [9] have been generalised and mapped upon the physical model, the domains.

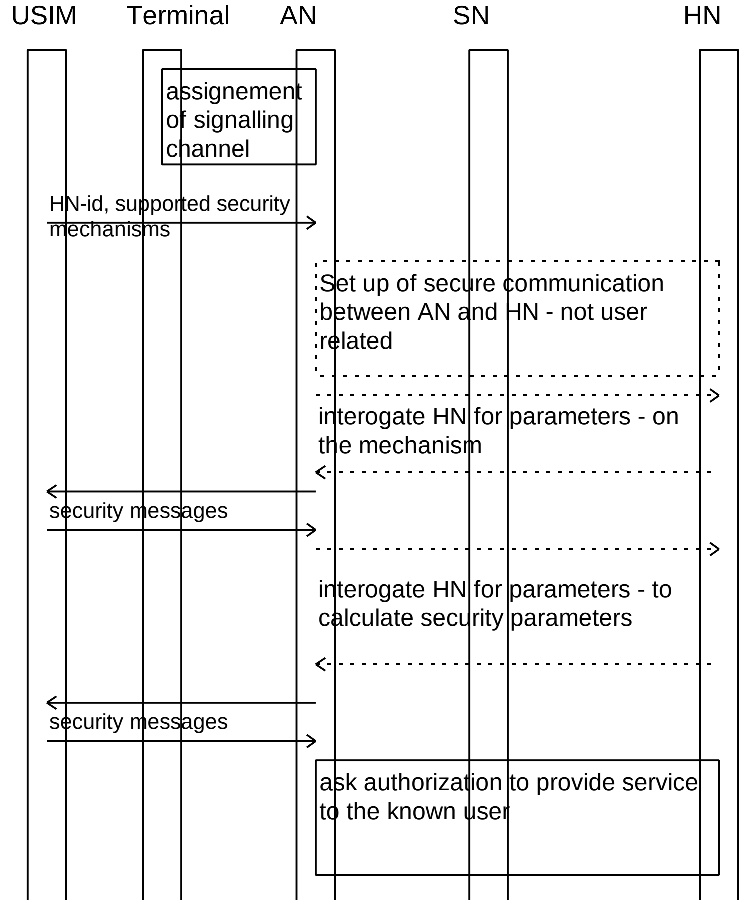
USIM
Terminal
AN
SN
HN
assignement of signalling channel
HN-id, supported security mechanisms
Set up of secure communication between AN and HN - not user related
interogate HN for parameters - on the mechanism
security messages
interogate HN for parameters - to calculate security parameters
security messages
ask authorization to provide service to the known user

Figure 4 User security procedure[2]

[2] The dotted line indicate actions or messages that can be omitted, when certain preconditions are set.

The request for authorisation to the HN only has to occur if the user initiated the contact. Authorisation has to be retrieved for the use of the services in the specified AN. In addition the preferred Serving network has to be indicated by the HN. The HN has to achieve the best buy for the user. This can be different depending on the asked service.

The communication between the AN and HN is supposed to be authenticated (and confidential ?). This is completely user independent.

There can be a need by the AN to interrogate the HN, to retrieve more information (e.g. missing parameters) on the security mechanism. This is user independent, but different mechanisms can be in use by groups of users of a specific HN.

During the security procedures, there can be a further need by the AN to interrogate the HN for security data (e.g. response parameters, that can be calculated only in the HN). This is a user dependent interrogation.

When the user is already known in the AN, the procedure can be simplified and good real-time procedures will no longer need an interrogation of the HN and fewer data to be transferred.

What should security procedures achieve ?
1. mutual authentication
2. setting of a cipher key between the Mobile and the AN
3. anonymous user access
4. non-repudiation of access of service
5. initialisation of on-line billing process by means of micro-payments (between the mobile and the HN)

At the end of a successful authentication sequence a cipher key is set between the AN and the smart card. This cipher key can be used to cipher the connection between the mobile terminal (ciphering is still not feasible within the smart card, due to the limited transport speed between the smart card and the Mobile, 55kbits/sec) and the AN.

The described procedure has to guarantee perfect user anonymity. An example of a procedure : setting of a cipher key during a public key based authentication mechanisms, followed by the ciphering of the real identity with the cipher key.

When at a following contact, ciphering needs to start asap[3], without authentication, a temporary identity can be used during this procedure. This temporary identity needs to be transmitted ciphered. The user can use that temporary identity unciphered one time for identification. The AN and mobile terminal can start ciphering immediately and assign a new temporary identity and transmit it ciphered to the MS.

7.3.Conclusion

The authentication framework can be used within the UMTS architecture currently defined. More work has to be done to integrate the authentication framework with the signalling procedures generated for UMTS. In addition it has to be enhanced to support more security mechanisms, especially for non-repudiation of billing, on-line billing and support for electronic commerce.

[3] This is also required when transmission is packet oriented.

8.Conclusion

This deliverable evaluated the authentication framework as a basis for a migration scenario. The principle objective of the Authentication framework '**to provide a flexible procedure for user-network authentication allowing a number of different mechanisms and algorithms to be incorporated, with the ability to migrate smoothly from one mechanism to another'** is fulfilled. During evaluation topics were encountered, where further work is necessary and which are not covered by this project:

- Within UMTS society (SMG and UMTS forum) the service requirements changed, more value is now given to the 'support for electronic Commerce' and 'incontestable charging'. The security implications of having a UMTS network supporting electronic Commerce have not been studied. Neither has there been done effort to integrate incontestable charging protocols within the basic UMTS mechanisms. Within the secure billing work package from ASPeCT a micro payment protocol has been developed to be used on application level.
- It is clear at the moment that for UMTS more and more use will be made of packet based services. The authentication framework with the explicit authentication mechanism can not fulfil the packet based requirements. Security has to be guaranteed on a packet based level. No work has been done on the introduction of appropriate security mechanisms for packet based services.
- Within the ASPeCT project the evolution from the UMTS architecture has not been studied. At the start of the project the role model defined in the former SMG5 has been taken as a starting point. An evolution towards a domain/strata model in SMG3/SA was not expected. The model, currently available in SMG lacks the description of any security functions. The authentication framework has to be placed within the appropriate domain/strata in the UMTS architecture. More work has to be done there.
- ASPeCT has not studied the integration of the authentication framework within the UMTS signalling procedures. At the start-time of the project these procedures were not available, and even now the biggest part of the work has still to be done.