Secure Provision of UMTS Services over Diverse Access Networks

John Charles Francis[1], Holger Herbrig[2], Nigel Jefferies[3]

Abstract

This paper addresses the secure provision of UMTS services in diverse access network and is based upon the research work of the ACTS projects EXODUS, COBUCO and ASPECT. One of the distinguishing requirements of UMTS is that it should provide service in a number of distinct environments. This will necessitate the development of distinct radio interfaces for each environment, and a service provision and management functionality that can operate across diverse access technologies. Projects within the ACTS programme are addressing these issues, and we highlight the UMTS platforms developed by the COBUCO and EXODUS projects. The EXODUS services, access network, IN-based functional architecture and mobility management are described, which address the deployment of UMTS services through wired (ATM) and wireless (DECT) access networks. This is followed by a description of the services, access network and mobility management in the COBUCO project, where the emphasis is on the deployment of UMTS services in private networks using DECT access. Both projects are studying the practicability of selected UMTS services as demonstrated in an operating trial system.

Having described these platforms, we focus on the security issues raised by UMTS. These are being studied by the ASPeCT project, and we discuss how the security features developed are being integrated into the UMTS platforms. The focus here is on the joint trials scheduled with the EXODUS project.

Index Terms—UMTS, authentication, security, B-ISDN, ATM, DECT

I. Introduction

Third generation mobile systems supporting UMTS radio access will offer a wide range of telecommunication services including voice, video and data as well as more complex multimedia services. In line with the ETSI GMM report [1], such services may be provided in both public and private environments via a number of potential access networks including fixed B-ISDN/ATM, existing mobile GSM and DECT access networks, and new access networks specific to UMTS. The theme of this paper is the provision of UMTS services through these diverse access networks in a secure manner.

The evolution path from second generation systems towards UMTS has been investigated within the ACTS project EXODUS (Experiments on the Deployment of UMTS) and COBUCO (Cordless Business Communication Systems). While EXODUS concentrates on the deployment of UMTS services [2], COBUCO focuses on the installation of a communication island in a business environment for both service demonstration and usage of the advanced technology.

The provision by the network of call and mobility control that operates across a number of types of access networks is an issue that both EXODUS and COBUCO address.

The need for the provision of security features is also recognized in [1], in particular to deal with the additional threats inherent in a mobile network. Many of these threats also apply to the provision of personal mobility in fixed networks. But the more sophisticated digital mobile networks (such as GSM now and UMTS in the future) also have the opportunity to provide users with additional security services based on the use of the SIM or UIM - the smart card used to represent the user to the network.

II. ACTS Project EXODUS

The EXODUS project investigates experimental 3rd generation mobile system deployment by implementing mobile multimedia services in ATM networks with radio access based on DECT (*Digital Enhanced Cordless Telecommunications*) and B-ISDN fixed access. *Intelligent Network* (IN) techniques are used to manage personal and terminal mobility as well as advanced call-related signaling. User trials are scheduled in Switzerland and Italy, with the support of an ATM link between the Italian and Swiss ATM national host infrastructures. Mobile multimedia services in health care (hospital) and other environments will be demonstrated.

A. EXODUS Services

The EXODUS platform supports the following services:

Broadband Videotelephony: This is a real-time multimedia conversational service enabling two geographically separated users to exchange high quality voice and video.

Multimedia Information Retrieval: To support this service a workstation is used as a repository of encoded video clips and stills.

Database Access: Multimedia databases are provided.

Videotelephony over DECT: This is a real-time multimedia conversational service based on ITU-T recommendation H.324 using enhanced DECT radio access to the EXODUS network. The available bit rate is up to 384 kb/s.

Telemonitoring: Remote access is provided to real-time data sources for routine monitoring of cardiac activity and emergency health care intervention.

[1] Swiss Telecom PTT, R&D, Mobile Communications / FE423, CH-3000 Bern 29, Switzerland. Phone: +41 31 338 02 04 Fax: + 41 31 338 51 74 Email: JohnCharles.Francis@SWISSTELECOM.COM

[2] Alcatel SEL. Phone: +49 711 869 324 52. Fax: +49 711 869 324 35. Email: hherbrig@rcs.sel.de

[3] Vodafone Ltd, The Courtyard, 2-4 London Road, Newbury, Berks, RG14 1JX, England. Phone: +44 1635 503883. Fax: +44 1635 31127. Email: Nigel.Jefferies@vf.vodafone.co.uk

The applications will be demonstrated in two user trials:

Health Care Trial: Mobile multimedia services and telemonitoring will be deployed on movable hospital bed units and terminals at the University Hospital of Basel (Switzerland). The units and terminals are connected to an ATM switch by multimode optical fibers and a computer-based multimedia health-care application is supported.

Mobile Multimedia Trial: Mobile multimedia applications will be investigated with demonstrations of personal mobility between Italy and Switzerland. The applications include:

Data Retrieval: A database server will store business and professional information in the form of video and audio data. A user sets up a call to the server to access the data in a store-and-play fashion.

Direct Playing: Access is provided to MPEG-2 encoded videos stored in a *Multimedia Information Retrieval* (**MIR**) server. Under IN-control, a video and control-connection is set up between the terminal and the MIR server. The list of the MIR videos appears on the user's screen and one can be selected. The MPEG-2 encoded stream is transmitted in real-time over the video-connection and the user can manipulate the MPEG-2 playback through a control menu. Commands like Forward, Rewind, Stop and Pause are provided.

Collaborative Work: Videotelephony, data conversation and database access are supported. A face-to-face dialogue can be established and users can exchange multimedia documents. Data, graphics, audio, text or picture files can be transferred over a separate channel. Remote files can be uploaded and downloaded as required.

B. Access Networks

The platform for the EXODUS experiments is shown in Figure 1.

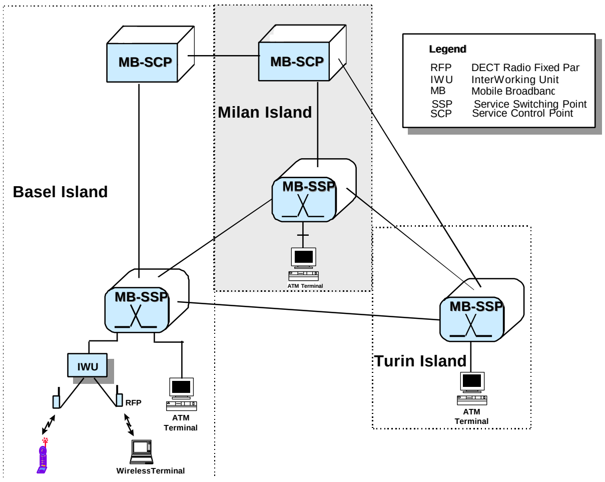


Figure 1: The EXODUS experimental platform

It consists of an ATM network based on the Swiss and Italian nation host infrastructures. Local ATM switches have been enhanced with IN functionality (MB-SSP) and service control is provided by two Mobile Broadband Service Control Points (MB-SCP's). These provide the logic for UMTS mobility support and services.

Access to the EXODUS platform is provided via enhanced *DECT* terminals (for wireless access*)* and *Fixed Broadband Terminals* (for wired access). The terminals contain UMTS functional entities which interact with UMTS application software via a UMTS Application Programming Interface (API).

In the case of DECT, an *Interworking Unit DECT/UMTS* **(IWU)** supplies the necessary functions for DECT-UMTS interworking on both the control and user planes. It ensures that the enhanced DECT terminals appear to be UMTS terminals when viewed from the perspective of the core network. In EXODUS, interworking is also placed inside the terminal to fully encapsulate the DECT access and allow software applications to be supported by a consistent UMTS-API in both wired and wireless terminals.

Other equipment includes a *Multimedia Information Retrieval Server* **(MIR)** which acts as a repository of multimedia data. The terminals and servers at the Basel and Milan sites are shown in **Error! Reference source not found.** .

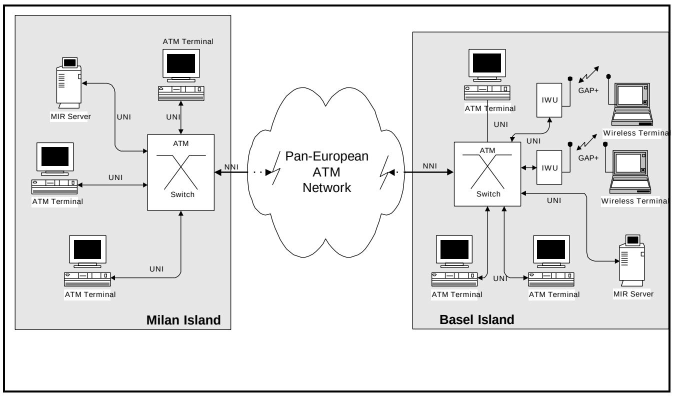
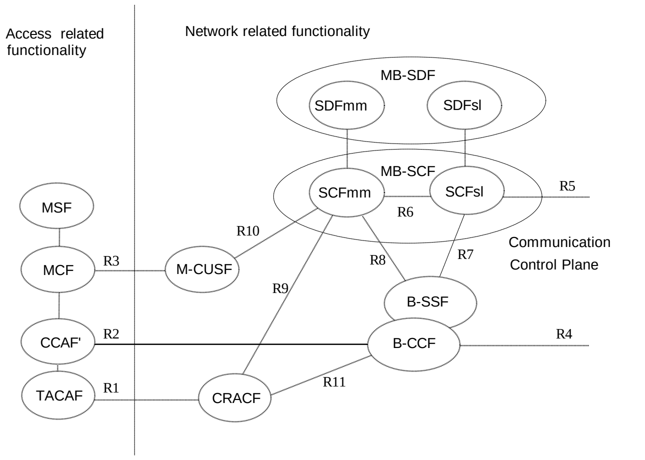


Figure 2: EXODUS Platform

C. An IN-Based Architecture for UMTS Service Support

The EXODUS project has specified an IN-based functional architecture for UMTS service support. The architecture, derived from ETSI work on Cordless Terminal Mobility (CTM) and ITU-T work on FPLMTS is shown in Figure 3.



Legend
SCFmm Service Control Function for Mobility Management
SDFmm Service Data Function for Mobility Management
SCFsl Service Control Function for Service Logic
SDFsl Service Data Function for Service Logic
B-CCF Broadband Call Control Function
B-SSF Broadband Service Switching Function
M-CUSF Mobile Call Unrelated Service Function
CRACF Call Related Access Control Function
MSF Mobile Service Function
MCF Mobile Control Function
CCAF' Enhanced Call Control Agent Function
TACAF Terminal Access Control Agent Function

Figure 3: The EXODUS functional architecture

The functional entities in the *network* are as follows:

1. The *Mobile Broadband Service Control Function* (**MB-SCF**) corresponds to the SCF defined in the ITU-T Q.12xx series, with enhancements for supporting mobile multimedia services in a broadband environment. To cater for concurrent service and mobility support, it is split into an **SCF$_{\mathbf{sl}}$** for control of user services and an **SCF$_{\mathbf{mm}}$** for mobility management. The SCF$_{sl}$ functionality includes user service support (e.g. call forwarding), subscriber

authentication, and control and allocation of resources for multimedia call set-up. The SCF_{mm} functionality includes mobility management.

2. The *Mobile Broadband Service Data Function* (**MB-SDF**) corresponds to the SDF defined in the ITU-T Q.12xx series. It is split into two parts the SDF_{sl} and SDF_{mm} which represent the database support for the SCF_{sl} and SCF_{mm} respectively.

3. The *Broadband Call Control Function* (**B-CCF**) handles B-ISDN calls and all the call-related interaction between the user and the network. It has the capability to detect call and bearer related events of relevance for the IN-service logic.

4. The *Broadband Service Switching Function* (**B-SSF**), in association with the B-CCF, provides the set of functions required for interaction between the B-CCF and the MB-SCF. The B-SSF extends the logic of the B-CCF to include recognition and correlation of service control triggers, and to interact with the MB-SCF. It manages signalling between the B-CCF and the MB-SCF, and modifies call/connection processing functions (in the B-CCF) as required to process requests for IN-services.

5. The *Mobile Call-Unrelated Service Function* (**M-CUSF**) handles requests from the MCF and routes to the SCF_{mm}. It also handles the SCF_{mm} response and routes to the MCF.

6. The *Call-Related Access Control Function* (**CRACF**) handles paging and authentication messages initiated by the SCF_{mm}. Routing is made according to a Location Area Identity (LAI) and point of attachment (POA). In the case of paging, the POA is not known and the message is broadcast at all POA's in the indicated location area; a specific terminal (TMTI) and user (TMUI) is addressed, and the TACAF responds with a paging status at a specific POA. The CRACF also routes responses from the TACAF to the SCF_{mm}.

The EXODUS functional entities in the *terminal* were derived from consideration of the FPLMTS functional architecture. They are as follows:

1. The *Mobile Control Function* **(MCF)** represents the service logic and service-related processing in the terminal. It supports the mobility functions (e.g. location management) and provides local service control. It sends messages via the M-CUSF to the SCF_{mm}.

2. The *Mobile Storage Function* **(MSF)** represents the data storage function in the terminal for support of the MCF. Data can be stored in the terminal or in a personalised smart card referred to as the User Identity Module (UIM).

3. The *Call Control Agent Function (enhanced)* **(CCAF')** represents the agent between the terminal applications and the network call control functions. It interacts with application to establish, maintain, modify or release calls. It interacts with the B-CCF to manipulate and release calls.

4. The *Terminal Access Control Agent Function* **(TACAF)** receives and responds to paging messages, broadcast via the CRACF, which are initiated by the SCF_{mm}. It also handles authentication messages.

D. Mobility Management

The following *call-unrelated* mobility management procedures are supported by EXODUS:

Location Registration: This procedure is initiated by the wired, movable or wireless terminal, whenever it enters a network or if the stored location information is lost. The terminal with a first user registered on it notifies the network of its location. The first user can register on a terminal for incoming calls, and/or for outgoing calls.

Location Deregistration: This procedure is used to deregister all users from a terminal and to deregister the terminal.

User Registration: This procedure is only required for terminals that support multiple users and is used to register a subsequent user on a terminal. The first user is registered by location registration.

User Deregistration: This procedure is initiated by the user to notify the network that he/she is no longer reachable at that terminal. When the last user is removed, the terminal is also deregistered.

Location Update: Location Update is initiated by a terminal changing its point of attachment within a DECT or wired domain. This occurs when a DECT terminal roams from one location area to another, or when a wire-line terminal changes its point of attachment.

Service Profile Interrogation : This procedure is initiated by the user to interrogate the personal "service profile".

Service Profile Modification : This procedure is initiated by the user to modify the "service profile".

EXODUS support the following *call-related* mobility management procedures:

(Look Ahead) Paging: This procedure is used before bearer setup to determine the point of attachment of a called user, and to find out whether the user is busy, the terminal is powered down or the user is otherwise not reachable.

Handover: This procedure allows an active call to be maintained while the physical channels supporting it are changed.

III. ACTS Project COBUCO

A. Overview and Introduction

Within the framework of the ACTS programme, COBUCO, a consortium of manufacturers, research institutes and universities, is developing and installing a UMTS demonstration and trial system following the following phased approach:

- connecting standard DECT equipment to an ATM switch by means of a Switch Adapter;
- introducing mobility into a modified DECT environment requiring a Mobility Server on the ATM side;
- introducing multimedia capability into the DECT environment by dynamic slot bundling;
- interconnection of two such islands by a EURO-ATM link;
- running tests, experiments and real usage on these islands.

Both DECT and ATM are well founded, powerful and promising technologies. Consequently, it is challenging to combine DECT as an access interface and ATM as a transport backbone system to achieve a new type of mobile and fixed communication system. Additionally, this idea is strongly promoted by the discussion concerning UMTS, multimedia, third generation equipment, etc.

Consideration of these issues resulted in a project aimed at the development, installation and use of a UMTS system demonstrator, the **COBUCO** system. **COBUCO** focuses on the business environment as one of the most important pan-European market segments for the introduction of UMTS [3].

COBUCO stands for Cordless Business Communication. The envisaged system will consist of a DECT/ATM based multimedia UMTS system offering cordless and fixed access. It is designed to allow different types of mobility and includes multimedia services of up to 256 kb/s across the air interface and 150 Mb/s across the fixed access respectively.

COBUCO will start from the 2nd generation equipment and migrate towards the 3rd generation by enhancements and new developments. Critical migration aspects will be the subject of accompanying research activities [4].

B. Access Network

The first system realisation step is the development and installation of a self-contained communication island (Figure 4).

The island is grouped around an **ATM Switch** with an external **ATM Signalling Unit** handling the standard call and bearer signalling procedures according to Q.2931. It is accommodated on a common workstation platform together with the **Mobility Control Server** which forms an add-on part to the **Signalling Unit** and handles all the features dealing in general with mobility in the network (such as registration, service profiles, location management, handovers) [5]. The introduction of mobile Internet protocols requires an additional **Mobile IP-Server** to manage the addresses of mobile Internet users.

The gap between the ATM and DECT worlds is bridged by the **ATM Switch Adapter**. This component terminates the ATM and DECT protocols and enables the interoperability of DECT and ATM. Additionally, the Switch Adapter handles all functions on lower layers (such as packetizing and routing).

The **Base Station** development is based on a DECT base station for speech application. It will be upgraded to a 4-slot-bundling version and finally an 8-slot-bundling prototype which will support higher data rates for multimedia applications of up to 256 kb/s in each direction.

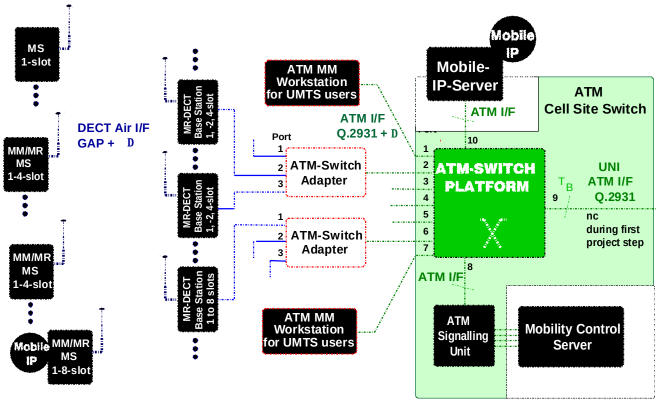


Figure 4: COBUCO communication island

The introduction of multimedia functionality and UMTS features requires additional or modified hardware, in particular **modified terminals**, and enhanced protocols. On the terminal side the existing simple DECT portables will develop into comfortable portable mobile stations consisting of a choice of laptops, phones, faxes, and so on, but later integrated in one item. A similar configuration can be applied to the fixed ATM terminal (called **ATM Multimedia Workstations** for UMTS users) but operating at a maximum bit rate of more than 100Mb/s. Both the mobile and the fixed terminal allow full personal mobility and terminal mobility restricted by the portability of the equipment.

C. System Migration

The second project step is aimed at the interconnection of the communication island to the "outside world" and subsequently of two **COBUCO** islands by, for instance, a Euro-ATM link. Both islands will be regarded as individual domains (that is, in the case of **COBUCO**, the islands may be installed in different company premises). Figure 5 depicts the second project step configuration.

The identification of the interconnecting system for these two **COBUCO** islands is still under consideration, mainly depending on the final location of the islands. The choice ranges from a pure (physical) ATM line to a comfortable ATM-capable host system. An intermediate step between the first and second project step will be the selection of the final location of both islands and the selection of an appropriate interconnecting network between these two islands [3].

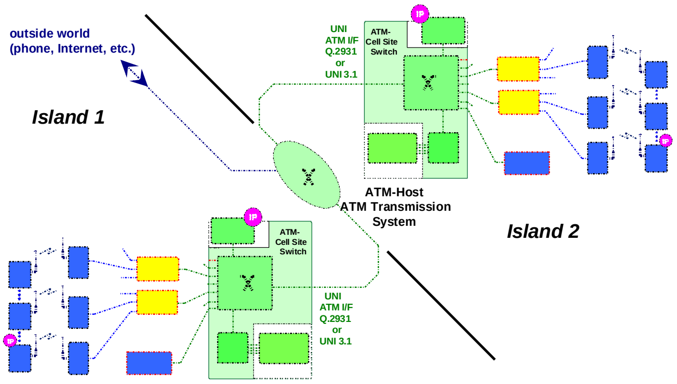


Figure 5: Envisaged interconnection of two COBUCO islands

D. Terminals

The DECT radio interface is a standard for a 2nd generation telecommunication system, fully defined by ETSI. This makes it a suitable testbed system for validating UMTS protocols in the migration towards a 3rd generation system. This consolidated standardisation level has encouraged **COBUCO** to develop a number of different DECT-based mobile terminals. To keep development resources to a minimum, terminal design will follow an upgrading principle; new prototypes can be developed by upgrading the available equipment during the project lifetime. Figure 6 indicates the envisaged migration path.

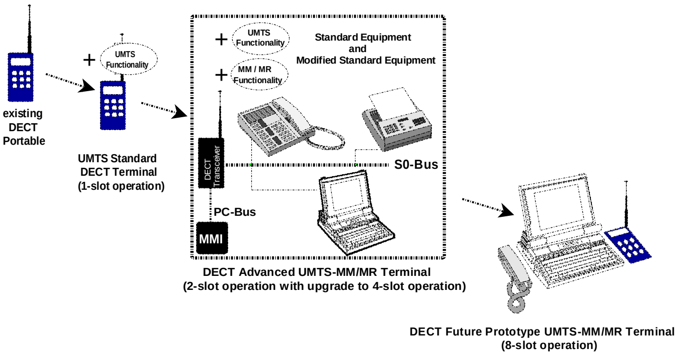


Figure 6: DECT UMTS terminals migration path

Initially, existing DECT standard mobile stations for speech application will be upgraded to a **"standard UMTS terminal"** that operates in one time slot with an enhanced DECT GAP protocol and so can fulfil an initially restricted set of UMTS requirements.

As a first intermediate step towards a multi-slot solution the mobile station is envisaged as a vehicle-mounted modular assembly of standard ISDN terminals together with a lap-top PC. The kernel is a DECT transceiver acting as an access point to standard S_0-terminals as well as a PC-ISA-bus. The lap-top may be connected to both the S_0 and the PC-bus, through which the PC fulfils all those additional tasks that allow UMTS capability of this equipment set and serves as the necessary MMI. The advantage of this architecture is that it allows the connection of more or less standard equipment. This configuration is called the **"DECT advanced UMTS MR/MM terminal".** For the first approach the multimedia terminal will be a multimedia laptop including DECT services.

It is obvious that due to low portability, the terminals described above allow only a restricted degree of mobility. Consequently, in a further step, a **"DECT future prototype UMTS-MR/MM terminal"** will address this problem. This terminal type will be capable of operating in 8 time slots and so increase the data rate to 256 kb/s [6].

E. Application Scenarios

Application scenarios for **COBUCO** are characterised by these features:

- application in a private business environment, where users belong to business, commercial, and professional groups;
- the exchanged information has a multimedia character, that is, it is expected to be a mixture of speech, image transmission, file transfer, interactive operations, and so on;
- the service area will be of suitable size so that DECT radio coverage will be sufficient;
- the application environment in which the **COBUCO** island is installed need not be stable and may change continuously (building sites, fairs).

The following application scenarios may be regarded as the main ones for **COBUCO**:

- business corporate networks;
- hospitals and universities;
- building sites and dockyards;
- aircraft, train and car maintenance.

F. Envisaged User Services

The definition of the final range of services to be implemented is an ongoing matter in accordance with the system architecture concepts, the protocol concepts, and requirements arising during the project and from contact with other projects within ACTS. Therefore the following paragraphs should be regarded as an incomplete list only [7].

With respect to the various application scenarios, a number of user services can be defined to make these scenarios work and allow professional use. The table below contains only initial ideas on services that are either self-evident to users (including basic services) or provide a good basis for multimedia and/or UMTS/UPT demonstrations and applications within the project.

Lap-D-supported services:	TCP-IP supported services:
- Telephony, Video Telephone	- Email (also for mobile users)
- Data Transfer, Fax	- FTP
- Short Message Services	- Remote Login
- Calling Line Identification	- Interactive Application Sharing
- ISDN Supplementary Services	- Internet Access
- Videotex, Paging	- Voicemail

All these services are characterised by the available bandwidth; for **COBUCO** it is obvious that the appearance and quality of services depends on the type of access, that is, whether a terminal is connected via the DECT multimedia multi-rate air interface or directly to the ATM line. Envisaged service classes for services over the DECT air interface are as follows:

service class	bandwidth	DECT	ATM
voice CBR	32 kb/s	1 single slot	1 AAL1
data CBR	64 kb/s	1 double slot	1 AAL1
data VBR	0...256 kb/s	1 to 4 double slots	1 AAL5
data CBR	< 64 kb/s	not part of **COBUCO**	

G. COBUCO Mobility Management

The Mobility Control Server of the **COBUCO** system is able to handle the mobility functions listed below. These functions reflect the actual implementation status; the server and its data base will in the end not be restricted to the items below:

- terminal attach/detach;
- user registration/de-registration;
- user session handling;
- service profile handling;
- change PIN;
- location management (user/terminal locating);
- intra-cell handover;
- inter-cell handover;
- inter-cluster handover.

IV. ACTS PROJECT ASPECT

A. Security in mobile networks

Adequate security features form an integral part of any mobile telecommunications system. In second-generation systems such as GSM and DECT, security features based on cryptographic techniques have been included in a systematic way for the first time. The increasing, and increasingly diverse, demand for security by users, operators and regulatory bodies calls for more advanced security features in third generation systems, such UMTS. The goal of ASPeCT is to specify such advanced features and verify their feasibility and acceptability as part of demonstrations and trials. Some of these advanced security features in UMTS, in particular the use of public key cryptography, will be made possible through the use of more powerful smart card technology and the availability of Trusted Third Parties (TTPs) acting as certification authorities for public keys.

Specific security objectives, requirements and a classification of security features have been developed by ETSI [8]. Mechanisms to realise the UMTS security features are currently under development. Secret key and public key based mechanisms have been proposed for UMTS, providing mutual authentication, cipher key agreement for confidentiality, anonymity and non-repudiation.

B. The ASPeCT project objectives

The technical work within ASPeCT comprises the following:

- Ensuring that migration from second generation systems to UMTS occurs in a secure way without jeopardising the quality of service or security of new or existing services. Secure interworking of different networks is required to allow roaming. A framework for authentication in UMTS has been established.
- Developing methods to detect fraud in UMTS [9]. Fraud scenarios and indicators are being investigated and developed. Legal and presentational aspects are also being considered.
- Proposing an international solution to the problem of managing keys to provide security services for mobile telecommunication use. This involves using a Trusted Third Party to deal with the secure management of cryptographic keys.
- Developing new ideas about, and assisting the smooth migration to, future User Identity Modules. This involves promoting improvements to smartcard technology and investigating user-to-UIM authentication based on biometric techniques [10]. To enable migration from GSM to UMTS a multi-application card has been defined, containing a GSM SIM application and a preliminary UMTS UIM application.
- Developing services supporting the security and integrity of billing in UMTS.

C. An authentication framework for UMTS

1. The Framework

The principle objective of the ASPeCT authentication framework [11] is 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. This framework allows the authentication capabilities of UIMs, network operators (NOs) and service providers (SPs) to be taken into consideration for the selection of the mechanism to be used. A list of capability classes (including the mechanisms supported) is maintained so that the different entities can permit the negotiation of the mechanisms to be used.

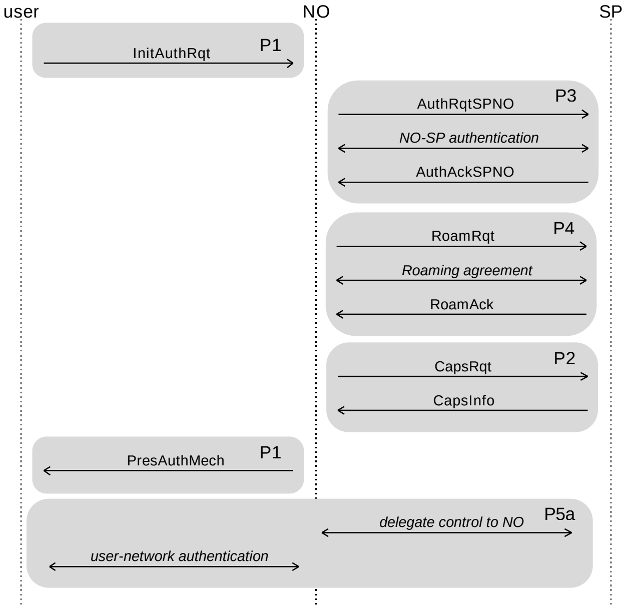


Figure 7: Operational scenario for 'User not registered, no roaming agreement'

To facilitate roaming in a network with many NOs and SPs, roaming agreements should be set up dynamically, as and when they are required. A roaming agreement would be requested after an initial authentication request sent by the user/terminal to an NO visited for the first time. A prerequisite is that the SP and NO involved have authenticated each other. This will be carried out using a globally agreed mechanism to ensure that all NOs and SPs have the capability to authenticate each other. Flexibility to change mechanisms is not a crucial factor. NO-SP authentication also permits the SP to delegate user-NO authentication to the NO.

The Authentication Capability Class (ACC) identifies the particular authentication mechanisms supported by the UIM. Each respective mechanism has a unique identifier. This is so visited NOs can immediately identify whether they can support a particular ACC; unknown mechanisms would be defined by the respective SP upon request from the NO.

2. An Operational Scenario

As an example, the operational scenario is shown in Figure 7 where a user, not registered in the network, initiates authentication and no roaming agreement exists between the NO and the user's SP.

D. Security services for users

1. Services using Trusted Third Parties

Trusted Third Parties (TTPs) allow users to establish confidential communication channels with other users, possibly in different countries, whilst being able to satisfy law enforcement requirements at both the national and international level by allowing the recovery of confidentiality keys under appropriate controls - such as an extension of a search warrant.

The ASPeCT TTP provides UMTS users with a mechanism to support end-to-end confidentiality of communications. In our model, two users who wish to communicate with each other make use of the key management services provided by a TTP infrastructure to support the establishment of a shared secret confidentiality key to be used in a symmetric cryptosystem. We assume that each user belongs to a *domain* (perhaps a country) and that they only directly communicate with a *home TTP*, which is a TTP associated with their domain.

An important feature of the mechanism is that some information used to generate the shared secret confidentiality key is escrowed to the TTPs. Thus, the demonstrator offers a mechanism whereby an *interception agent* can obtain the information, which may then be used to decrypt targeted communications.

The protocol used to establish a shared secret confidentiality key in the first demonstrator is based on the JMW architecture [12].

An ETSI Guide on Requirements for Trusted Third Party Services [13] describes six potential TTP security services, of which the ASPeCT TTP implements the two most important; key management services for asymmetric cryptosystems and key escrow/recovery services.

2. Secure billing protocol for UMTS

ASPeCT has developed a protocol to show how mobile users can pay for access to information services in a flexible, efficient and secure way. The method has potential application to charging for any telecommunications service.

It is expected that the number and variety of value added services (VASs) will greatly increase while current networks are evolving towards UMTS. The charging for today's VASs typically consists of a basic charge for the telecommunication service and a premium for the value added service. Both are usually based on the duration of the call. In the future, more flexible charging schemes for the premium would be desirable. Flexibility relates to the parameters which determine the charge, to the variety of different possible tariffs and to the ease with which a certain tariff can be changed.

The value of a particular piece of information retrieved by a user from a VAS provider at any one time may be quite small. Therefore, the use of computationally expensive payment mechanisms may not be acceptable. In addition, the scheme has to take into consideration the specific requirements of a mobile telecommunications system. In short, the charging scheme must be also efficient.

The evolution of current mobile systems towards UMTS will see the emergence of many new network operators, service providers and VAS providers. This will have serious implications for the trust relations among them. It will be increasingly important that the charging scheme is secure against cheating, and that parties involved should have the assurance that justified claims relating to charges can be proved and that unjustified claims cannot be successfully made. This is called incontestable charging.

Our approach is via a credit-based micropayment scheme based on tick payments [14].

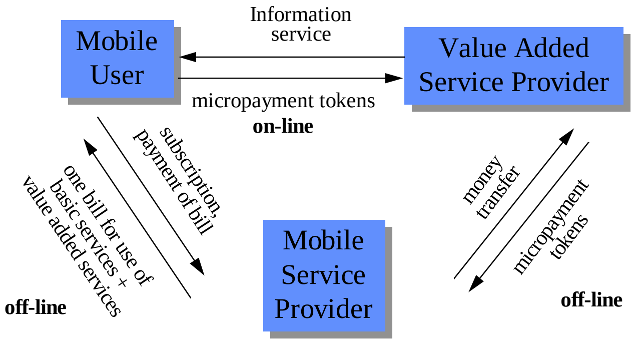


Figure 8: The ASPeCT billing model

In our model (see Figure 8) the user has a subscription with a UMTS service provider. The charge for using a VAS is composed of two parts:

- a basic charge for the provision of the communication link between the user and the VAS provider by the network operator and;
- a premium for the value added, paid to the VASP.

The subscriber enters into contractual relationship with the SP on behalf of the user. Any payment scheme for the protection of the premium has to be run between the user and the VASP. The fact that the network operator need not be involved has the advantage that the implementation of security enhancements to existing VAS requires no modifications to whatever network is providing the connection. The only changes which are necessary are software changes at the end-points of the communication. In this way, the solution is not restricted to UMTS.

The only on-line communication required in the charging procedure is that between the user and the VASP while the service is being provided. The VAS provider will forward the information proving his claims on the user to the SP (possibly through the NO) off-line who in turn will bill the user, also off-line. The SP will also take care of the payments to NOs providing the connectivity.

E. Integration of ASPeCT security features

To show that features and services developed are suitable for use in a third-generation system, ASPeCT are integrating them into the UMTS platform developed by EXODUS, and running a trial of the result. In fact, there are two trials, each requiring a different level of integration into the EXODUS platform.

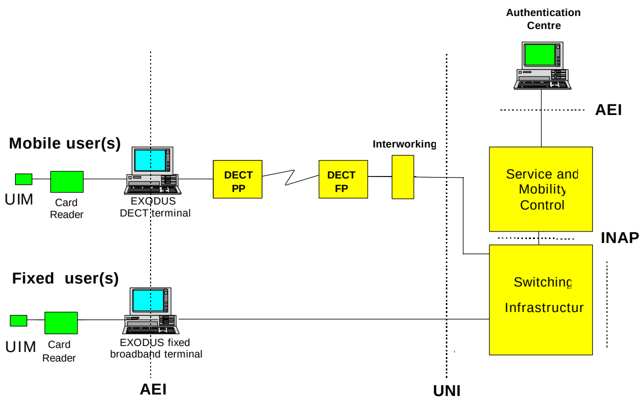


Figure 9: ASPeCT authentication trial

1. ASPeCT authentication trial

The ASPeCT UIM, authentication centre and terminal software are integrated with the EXODUS platform, so that users accessing the platform via DECT or fixed multimedia terminals will be able to authenticate themselves and the network.

ASPeCT-EXODUS interfaces (AEIs) are indicated in Figure 9, as are the elements provided by ASPeCT and EXODUS.

2. ASPeCT TTP/secure billing trial

ASPeCT security services (including the secure billing protocol) run as applications over the network.

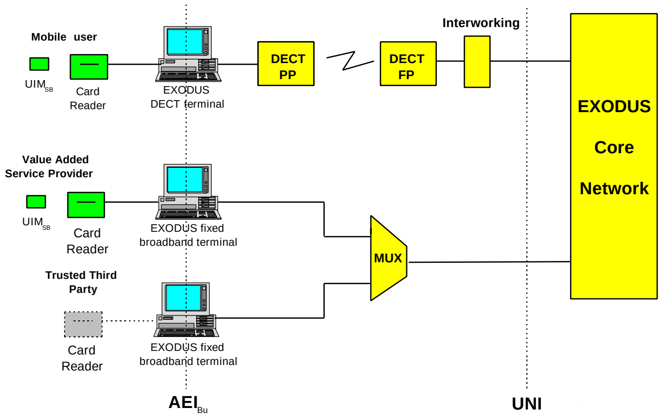


Figure 10: TTP, secure billing services and a value added information service (Phase 2)

The TTP and secure billing trial involves three ASPeCT entities: a mobile user, a Value Added Service Provider (VASP) and a Trusted Third Party (TTP). The mobile user has DECT access, and the VASP and TTP have fixed broadband access to the EXODUS experimental UMTS platform.

The configuration envisaged for the trial is shown in Figure 10 below. ASPeCT software will exist on the EXODUS terminal PCs. In both the DECT terminal and the fixed broadband terminal, a software interface will exist within the EXODUS terminal which separates ASPeCT and EXODUS functionality.

The configuration for the trial is shown in Figure 10.

V. Conclusion

In this paper we have investigated the secure deployment of UMTS services in diverse access networks, through the results of three ACTS projects. EXODUS considers the deployment of UMTS services in wired and wireless environments using an ATM network with IN-based mobility management. COBUCO focuses on the private environment with DECT and ATM support. ASPeCT addresses the security aspects inherent in UMTS service provision.

To ensure secure service provision, authentication is needed for all call-unrelated mobility procedures (with the possible exception of location update). Authentication is also required during UMTS call setup. But an initial authentication procedure is not in itself sufficient. Security procedures to protect the network and user must be sufficiently integrated into the network so that both signalling and user data can be protected. This contrasts with the so-called end-to-end security services, which can run as applications transparently over the underlying network. These issues are currently investigated within the context of joint trials scheduled between ASPeCT and EXODUS.

VI. Acknowledgements

We would like to thank all those participants in the ASPeCT, EXODUS and COBUCO projects who have developed the results reported in this paper. Partners in the projects are as follows:

ASPeCT: Vodafone Ltd, Siemens Atea, Giesecke & Devrient, Lernout & Hauspie, Panafon SA, Royal Holloway University of London, Siemens AG, Katholieke Universteit Leuven;

COBUCO: Alcatel SEL, Algosystems, Broadcom Eirann Research Ltd, Danish Electronics Light and Acoustics, Deutsche Forschungsanst. für Luft- und Raumfahrt, FORBAIRT, GMD Focus, Hagnuk Telecom, NTUA, Trinity College, University of Patras, University of Rome 'La Sapienza';

EXODUS: Italtel, Ascom Tech, Belgacom, CSELT, GPT, Intracom SA, NTUA, OTE, Philips LEP, Philips PRL, Swiss PTT, Syndesis, Telecom Italia, Teltec, TMR, University Hospital Basel.

VII. References

[1] ETSI PAC EG5, "Global Multimedia Mobility (GMM) – A Standardisation Framework," ETSI Board approved version, August 1996.

[2] J.C. Francis, A. Elberse, R. Gobbi, P. Rogl, M. Ciancetta, P. Monogioudis, J. Nelson. "Evolutionary Mobility & Service Support in DECT Access Networks". To appear in October '97 special issue of IEEE JSAC on Personal Communications - Services, Architecture and Performance.

[3] H. Herbrig, R. Rheinschmitt: "DECT/ATM Based UMTS Demonstration and Trial System", Proceedings of ACTS Mobile Telecommunications Summit, Vol.1, Granada, Spain, Nov. 1996; pp. 197-185.

[4] C. Delucchi, H. Bischl, T. Bregenzer, "Analysis of Multimedia Services and Traffic Models for the COBUCO System", Proceedings of ACTS Mobile Telecommunications Summit, Vol.1, Granada, Spain, Nov. 1996, pp. 405-411.

[5] J. G. Markoulidakis, E. P. Adamidis, D. F. Tsirkas: "UMTS DDB Optimization: Design Rules for Data Storage Nodes and Directory Tree Height", Proceedings of ACTS Mobile Telecommunications Summit, Vol.2, Granada, Spain, Nov. 1996, pp. 700-706.

[6] H.Flügel, S. Harder, J. Riechers, W. Weise: "DECT Mobile Terminals for Multi Slot Operation", Proceedings of ACTS Mobile Telecommunications Summit, Vol.2, Granada, Spain, Nov. 1996, pp. 778-784.

[7] ACTS AC031 COBUCO deliverable D02: "Protocol Concepts & Architecture"; A031/BRI/SNM/DS/P/D02/d1, July 1996.

[8] ETSI TR UMTS 33.20 'Security principles for the UMTS.' Version 3.0.0.

[9] P. Burge et al. 'Novel Techniques for fraud detection in mobile networks.' Proceedings of ACTS Mobile Telecommunications Summit, Vol. 1, Granada, Spain, Nov. 1996, pp. 231-234.

[10] E. Johnson, M. Lapère, User authentication in mobile telecommunication environments using voice biometrics and smartcards, Intelligence in Services and Networks: Technology for Cooperative Competition, IS&N '97 Proceedings, Lecture Notes in Comput. Sci. 1238, 1997.

[11] ASPeCT deliverable D17 - Migration scenario: final version. Ref. AC095/ATEA/W21/DS/P/17/1, June 1997.

[12] N. Jefferies, C. Mitchell, M. Walker. 'Combining TTP-based key management with key escrow.' Royal Holloway Computer Science Department Technical Report CSD-TR-96-10, 1996.

[13] ETSI Draft prEG 201 057 'Telecommunications security: trusted third parties (TTPs); requirements for TTP services', Edition 1.1.1, May 1997.

[14] T. Pedersen. 'Electronic payments of small amounts.' Technical report DAIMI PB-495, Computer Science Department, Aarhus University, August 1995.