User Authentication in Virtual Home Environment

Tuomas Kaipainen
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
tuomas.kaipainen@iki.fi

Abstract

Virtual Home Environment (VHE) lets users use the same set of selected services and a personal customized user interface when roaming in other networks or using different terminals. Authentication of the user and service providers is important as access to user profiles has to be tightly controlled. There are different methods for user authentication, in mobile systems a token/password combination is traditionally used. The paper presents a proposed VHE architecture built with agent technology. Other current work and ongoing VHE projects is also presented. Analysis is performed on the example architecture and other implementation proposals. Conclusions are then presented stating that security and authentication is generally not well thought of in prototype implementations and candidate architectures.

1 Introduction

1.1 General

Mobile networks are about to reach their third generation and are getting more and more mature. Network providers have made roaming contracts all over the globe to enable their subscribers to use their terminals in foreign networks. As the third generation of mobile networks and new terminals start to emerge a lot of new service types and categories also appear to market. Users also start to have more than one terminal connected to the network as new and different types of terminals emerge on the markets. The technical aspects of the terminals improve, high bandwith and larger color screens lead to a gigantic leap in the amount of services offered to users. From this multitude of services every user must pick the ones that are most useful to them. Methods to retain these selections over different networks or terminals are needed. When personal information of the users is stored for this in databases strong and secure authentication procedures are also needed in order to control access to this information.

1.2 Scope

This paper introduces VHE and the needs of authentication it has. Proposed solutions are viewed, analyzed and compared to see if and how they try to face these requirements. Example solutions are still on very early stage and no ready implementations of VHE exist

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

yet, so it is not possible to make final conclusions from this data. The paper does not go inside protocol implementations, an example of a public-key authentication protocol designed for third generation mobile communications systems is for example the one suggested by Günther Horn and Bart Preneel in [8].

2 Virtual Home Environment

2.1 General

The Virtual Home Environment (VHE) is a concept defined by 3rd Generation Partnership Project (3GPP), a collaboration agreement bringing together multiple telecommunications standards bodies[15]. VHE enables a mobile user to receive services as though the user would constantly reside in home network even when roaming in other networks. The user can have a personal service environment (PSE) that remains the same even when the user uses other networks than home network or uses other terminals. The personalised environment includes selected and personalised services and user interface customization. The used terminal can have limitations so that all the parts of the personalised environment are not available in all terminals. The VHE concept is designed for 3rd generation mobile networks (mainly UMTS), but it is meant to be applicable in all future networks and as a framework for implementing similar functionality to existing networks as well. [1] [12]

The scope of VHE includes providing a common access interface to services, enabling the creation of services and enabling the personalised environment to be recoverable. VHE consists of a Home Environment, users, Value Added Service Providers (VASP) and the personal service environment. If a VASP has an agreement with the home environment to provide services it is called a Home Environment Value Added Service Provider (HE-VASP). [1]

PSE consists of one or more User Profiles (UP) of which one can be active at a time. A user profile is a collection of information needed to provide the personalised service environment. The Home Environment offers users services to manage their user profiles and provides access to them for identified and authenticated users and also limited access to them for some VASPs. A value added service provider provides the various services for the users to use in their terminals. [1]

2.2 Authentication Requirements

VHE implementations should provide a secure environment for both the user and the home environment. The main thing to protect here are the user profiles. They could contain very personal and discrete information in the form of services that the user has selected to use and their confidentiality should not be compromised. The confidentiality level of the data may vary and the security level should be set according to that. Different levels of authentication must also be supported as users should typically have full access to their user profiles and HE-VASPs and VASPs only controlled and limited access. [1]

In 3GPP's VHE specification a list of required user profile security mechanisms is pre-

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

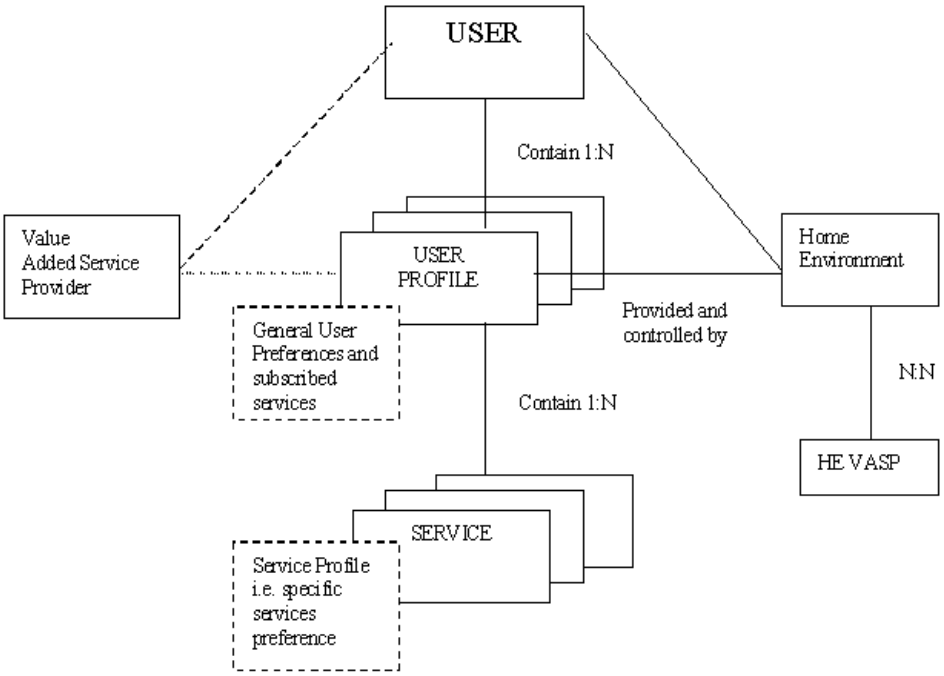

Figure 1: Logical VHE Role Model (User's View) [1]

sented. The ones related to authentication are as follows:

- The sender of data must be able to verify the authentication of the recipient before the actual data transfer.
- The recipient of the data must also be able to verify the authentication of the sender.
- It is allowed to use Trusted Third Parties (TTP) for authentication.
- It must be possible to set a validity time (a time after which the authentication expires and the authenticated party must re-authenticate) for an authenticated identity.

Requirements for confidentiality, data integrity, non-repudiation and audit logs are also defined. [1]

3 Mobile Authentication

Authentication is defined as the process of verifying a claimed identity. From this it follows that authentication is always linked to some identity. Authentication is usually used to give authorization, a permission to do or get something. Authorization can be anonymous and is not necessarily coupled with authentication.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

From the viewpoint of the user authentication can be based on: [6]

- Something you know (eg. a password)
- Something you possess (eg. a smart card)
- Who you are (eg. biometrics)
- What you do (eg. a signature)
- Where you are (eg. a specific terminal)

These can also be combined, an example being a password coupled with a possessed token such as a smart card[7]. In mobile systems this kind of token (SIM/USIM-card) coupled with a password (PIN code) is usually used. In GSM the token has been a SIM-card (Subscriber Identity Module). It is activated with a PIN code known by the user and can then be used as authenticating the user. In UMTS a USIM-card (Universal Subsriber Identity Module) is used [3]. The user and USIM similarly have a shared secret in the form of a PIN code that is securely stored on USIM. After the user has authenticated himself on the terminal the authentication to the network is transparent to the user. In UMTS the Home Enviroment sends a set of authentication vectors to the visited network and the authentication is based on a shared secret of the USIM card and the Home Enviroment[3]. A local authentication procedure is also defined if the user has previously been authenticated in the visited network.

USIM could also be used in VHE also to authenticate the user and to store user specific data and programs[9]. The terminal could however be almost anything just connected to a network so it is not clear that a USIM card can always be used. Authentication could also be just password-based.

Different proposed VHE architectures have their own solutions how authentication is passed on from the terminal to the home environment. Just like in all current mobile networks the home network entity, in case of VHE the Home Environment, needs always be contacted for authentication. For future networks beyond 3G research is being done to eliminate the home network as the single point of authentication for each user by employing Public Key Infrastructure Systems and Trusted Third Parties[5].

3.1 UMTS Authentication Architecture

An example of authentication in a mobile architecture is the UMTS security architecture. It is divided in different security feature groups. From the viewpoint of authentication the important groups are (numbered as in Figure 2):

- Network Access Security (I): Where the mutual authentication between the user terminal and the network is performed. Different parties here are the Mobile Equipment (ME), USIM card, Access Network (AN), Serving Network (SN) and the Home Environment.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

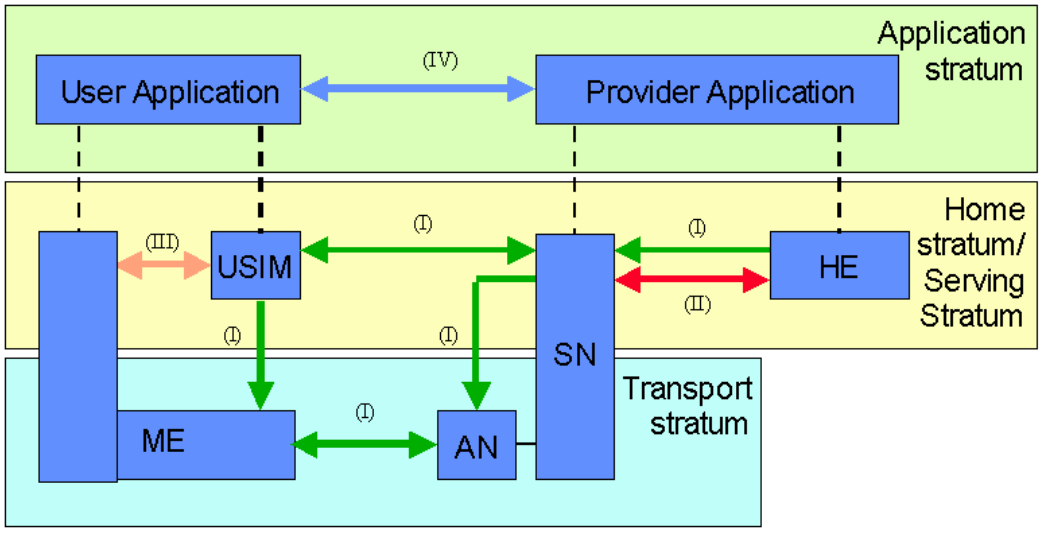

Figure 2: UMTS Security Architecture [3]

- User Domain Security (III): Where the authentication of user to the USIM is performed.
- Application Domain Security (IV): Is then concerned on the security of the communication between the user and services in the provider domain.

The user needs first to authenticate himself to the USIM-card for example with a PIN code and then the USIM and the network perform mutual authentication. The security features between the applications in user domain and in provider domain are largely undefined. [3]

4 Methods of Authentication

Various VHE implementations have been suggested and are in development. Most of them are still only initial suggestions or the implementations are not yet ready.

4.1 Open Service Access

The VHE can make use of several service toolkits, 3GPP or non-3GPP. One of the existing 3GPP toolkits is the Open Service Access (OSA, previousyly Open Service Architecture). The OSA toolkit may be used by the Home Environment, by VASPs and HE-VASPs. The OSA API offers an authentication function that an application and Home Environment can use to authenticate each other. The OSA is the architecture that enables the use of network capabilities by applications. The OSA authentication model is a peer-to-peer model, both parties need to perform their own authentication and both have to be authenticated before other OSA API functions can be used. OSA is described in figure 3. [2, 11]

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

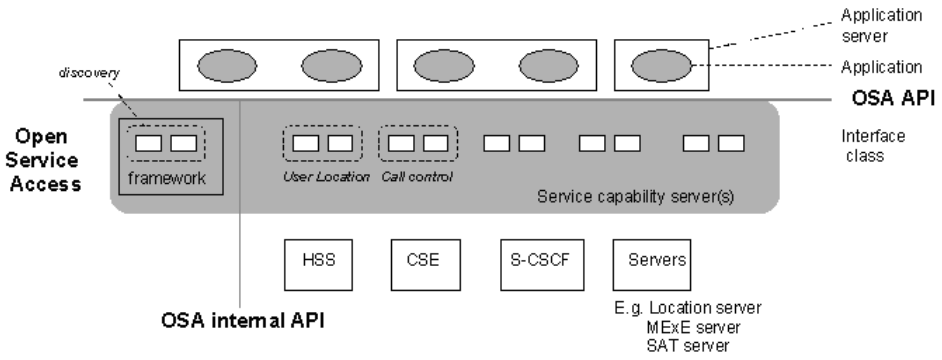

Figure 3: Open Service Access [2]

Once the initial contact between the application and OSA has been made for example through a URL or some naming service an appropriate authentication method is selected with the OSA API. Depending on the method also strong authentication techniques can be used and a minimum key length enforced. [2]

4.2 A Proposed Architecture

Larbi Esmahi, Roger Impey and Ramino Liscano suggest in their paper an architecture for providing mobile integrated services for roaming users. They suggest an architecture based on intelligent agents migrating from the VHE server to user terminal and to the service provider combined with universal user profiles. It maintains a universal user identity for authentication. [4]

A Terminal Agent (TA) provides an interface for authentication. A VHE-M agent residing at the VHE server performs the actual authentication and manages the database of user profiles. VHE-M should assure the consistence of both user and service profiles. When starting a VHE session it is first checked whether the terminal already has a TA in his cache. If a cached agent exists the version is checked and an outdated agent is replaced with a new one. If no cached version exists a new TA is sent to the terminal. Then the user can perform the authentication procedure using the interface provided by TA. [4]

After a successful authentication the VHE-M sends the user a User Profile Agent (UPA) to the user. The UPA contains the user information and provides together with TA an interface to the user for user profile management. When closing a session the TA communicates this to VHE-M agent and if the terminal has free resources both the TA and UPA are cached on the terminal. Authentication parties are presented in figure 4. The architecture also contains a Service Provider Agent (SPA) that handles the registration of services and a Service Interface Agent (SIA) that manages the communication between the terminal and the SPA. [4]

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

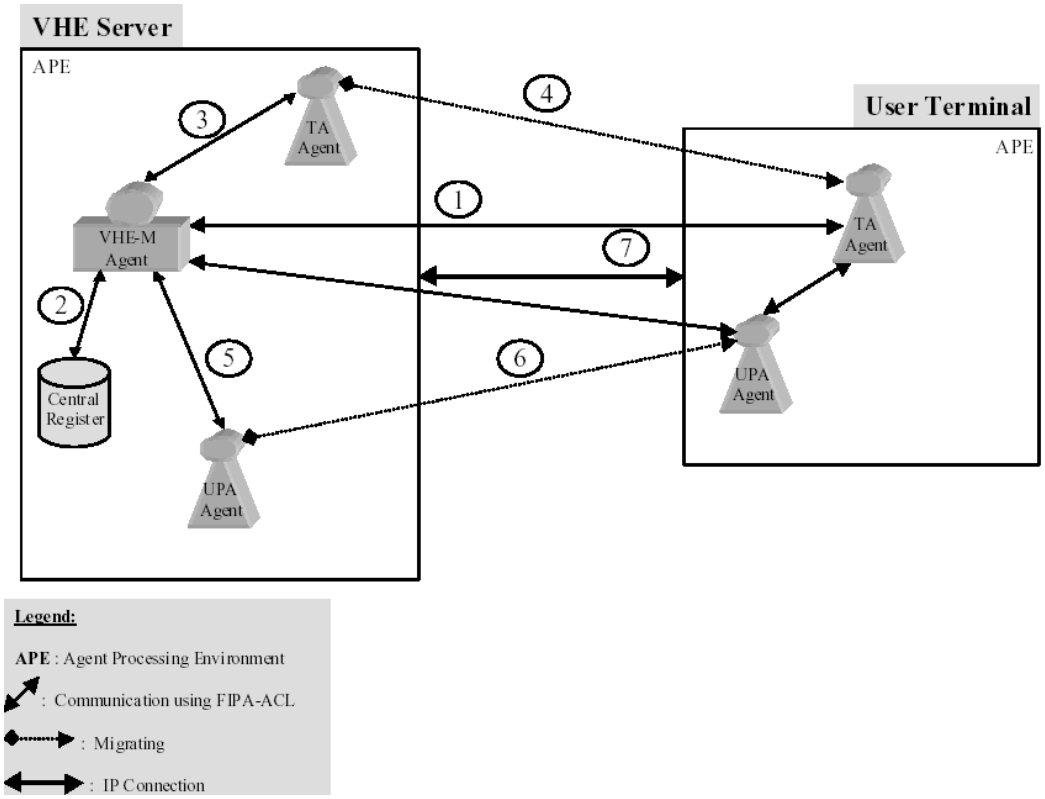

Figure 4: Starting a VHE session: authentication [4]

4.3 Other Work

The VESPER (Virtual Home Environment for Service Personalization and Roaming Users) project aims to design an architectural framework for VHE and to build prototypes in order to demonstrate and validate the framework. The final version is supposed to be completed in December 2002. VESPER kernel contains a specific module responsible for authentication and other security procedures. This Authentication/Security (A/S) Component handles the authentication of both the users and (HE) VASPs. The A/S Component has its own database for authentication data. User's authentication request is passed to A/S through Access Component. VESPER uses the OSA API to talk with the network, other external interfaces are the User API and the Service API. The authentication components and their relation to other components can be seen in figure 5 as Auth/Secur and Access. [13, 14]

Project P920 at Eurescom, the European Institute for Research and Strategic Studies, has built a VHE trial implementation[10]. They do not however tackle authentication issues at all but only use a simple password scheme with their WWW-based prototype. In general there seems to be VHE architecture discussion and ongoing trial projects but very little effort on considering security or authentication has been made.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

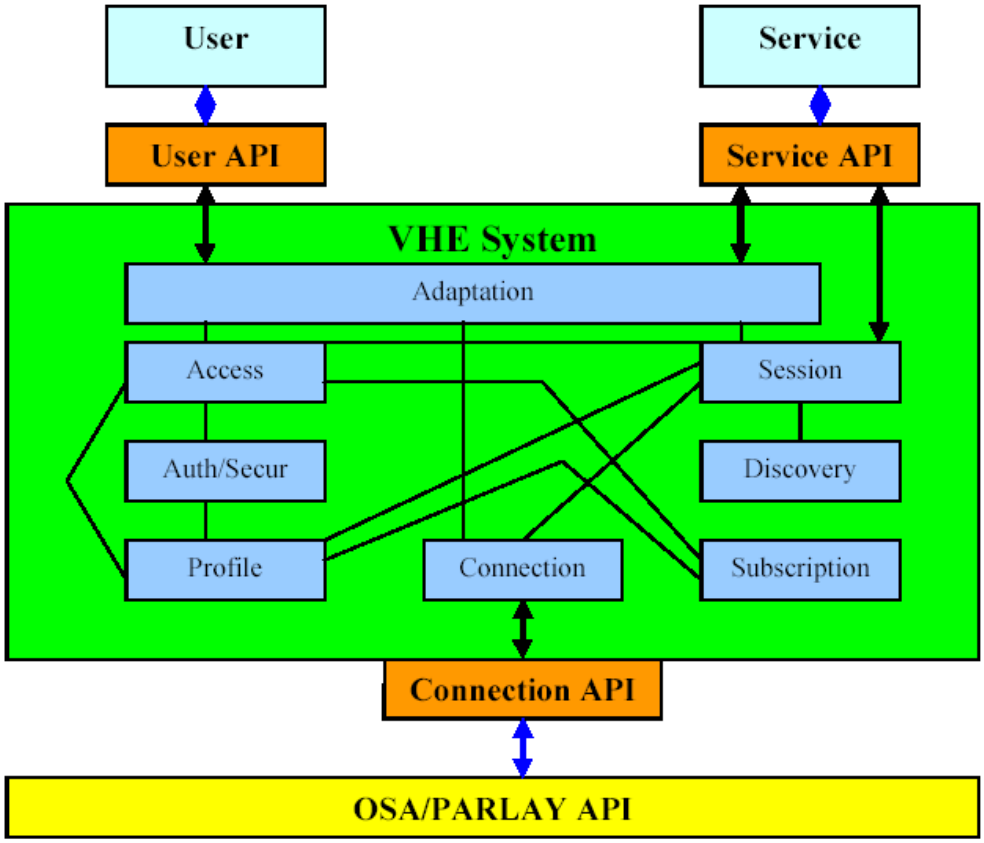

Figure 5: VESPER kernel architecture

5 Analysis

Authentication in VHE needs to be performed in different networks over different kind of terminals. These include mobile phones, PCs, different kind of PDAs and so on. As stated in mobile communications a (U)SIM card combined with a PIN-code is traditionally used to authenticate the user. VHE authentication solution needs to be universal and applicable with all different terminal types with or without an USIM-card.

The agent architecture of Esmahi et al. can be seen as a highly modular solution. They conclude that with the architecture the service provisioning and the customable look-and-feel of the services can be easily realised with their agent architecture [4]. However they only present the authentication of a user by the VHE server. VHE requires the user also to authenticate the server. Also access of the user profiles by VASPs and HE-VASPs is not discussed and also these issues should be tackled in the next phase.

The first phase of VESPER does not define any more elaborate authentication procedures and the authentication part can be considered fairly limited. This is also true with other on-going implementation projects and discussions. It seems that at the first phase of prototype implementations security is overlooked and simple schemes selected.

The authentication requirements of VHE state that mutual authentication of both the user and the visited network should be obtained. As authentication is not considered in the studied papers it would seem that the underlying network is trusted to perform the needed authentications. VHE requires however not just the authentication of user to the network but also to all the various VASPs and controlled access to the user profiles. As all kind of different terminals can be used an USIM-card is not necessarily always available and different network types could be used. In a VHE implementation that is going to be used in production a secure and verified authentication architecture should be explicitly defined.

6 Conclusion

VHE allows users to access their selected services and their personalized service environment and user interface when roaming in different networks or using different terminals - ubiquitous access to services. As we have seen that requires information of the users in form of user profiles, that have to be accessed not just by the users themselves but also by the service providers.

The concept of Virtual Home Environment is quite new and the work that has been done on the area is quite incomplete, ready implementations do not exist. At the early stage of an implementation everybody more or less seems to ignore security and authentication issues and concentrate on the more challenging and new issues. This is unfortunate as one of the key elements from user's perspective is the security of the user profiles and the knowledge that the system can be used without personal possibly sensitive information leaking into wrong hands.

References

[1] 3rd Generation Partnership Project Technical Specification Group Services and System Aspects, Service Aspects; The Virtual Home Environment In *3GPP TS-22.121 v5.2.0 12/2001*

[2] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects, Virtual Home Environment/Open Service Access In *3GPP TS-23.127 v5.0.0 12/2001.*

[3] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects, 3G security; Security Architecture. In *3GPP TS-33.102 v4.3.0 12/2001.*

[4] Esmahi L., Impey R., Liscano R. *An Architecture for Providing Mobile Integrated Services for Roaming Users.* Micont'00 24.-25.08.2000. http://micmac.mitel.com/resources/Esmahi.pdf

[5] Gehrmann Christian, Horn Günther, Jefferies Nigel, Mithcell Chris. *Securing Access to Mobile Networks Beyond 3G.* IST Mobile Communications Summit 2001. http://www.mobilesummit2001.org/mcs2001/papers/MOBCS4VYJM6.pdf

[6] Gollmann, Dieter. *Computer Security.* John Wiley & Sons 1999.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

[7] Halonen, Teppo. *Authentication and Authorization in Mobile Environment.* Seminar on Network Security, HUT TML 2000.

[8] Horn Günther, Preneel Bart. *Authentication and Payment in Future Mobile Systems.* http://citeseer.nj.nec.com/82814.html

[9] Kanerva et al. Project Eurescom P920-GI. UMTS Network Aspects. Deliverable 1 - VHE concept description, scenarios and protocols. June 2000.

[10] Mezquita et al. Project Eurescom P920-GI. UMTS Network Aspects. Deliverable 4 - VHE Trial View Report. June 2000.

[11] Stretch, Richard. *The OSA API and other related issues.* British Telecommunications Technology Journal Vol 19 No 1 January 2001. http://www.bt.com/bttj/vol19no1/stretch/stretch.pdf

[12] Vanhala, Anne. *Virtual Home Environment / Open Service Architecture*. 581385-2: Advanced Wireless Communications Systems, University of Helsinki 2000.

[13] Vesper Public Deliverables D11. *Project Presentation.* 3.11.2000 http://vesper.intranet.gr/DELIVERABLES/D11.htm

[14] Vesper Public Deliverables D32. *VHE Architecture Kernel Specification.* 6.4.2001 http://vesper.intranet.gr/DELIVERABLES/D32.htm

[15] www.3gpp.org.