An Ontology for Generic Wireless Authentication Data

Asma Alazeib, Andreas Diehl - Alcatel SEL AG, Germany

***Abstract*—Centralized, wireless subscriber profile databases access different network types and require a common data model. The data model has to unify the semantics of each access network. This paper describes an ontology for wireless authentication data of a centralized, next generation profile register. The approach is generic to telecommunications providers, because all the main wireless networks are supported. The ontology also aims to support the integration of future authentication methods.**

Data Model, Ontology, Protégé, Wireless Authentication

I. Introduction

Today wireless networks are separated and specialised for the requirements of each network provider. However, almost every telecommunications operator provides Wireless LAN (WLAN), GSM [1] [2] [3] and UMTS [4] [5] [6] networks to subscribers. Network applications use location-dependent, distributed subscriber profiles and specialised data models. WLAN services and dedicated data models are not standardised and mobile networks only use 3GPP standards for interface, protocol and service definitions. The data model of concrete wireless networks is independent from service description and its dedicated interfaces. Concrete data models for subscriber profiles are vendor-dependent in all relevant database technologies. Distributed subscriber profiles and different data formats complicate data integration. Therefore the need of integrating a centralized subscriber profile, which is completely independent from the access network, arises. Protégé/OWL is a technology which offers the possibility of describing all access networks on a logical level in a semantic way. The semantic description identifies dependencies and reusabilities of different subscriber profiles. Thus the ontology can be mapped to a concrete format to support an implementation of the semantic description. As an example the authentication data of different authentication methods are modelled.

Manuscript received April 4, 2005.

Asma Alazeib is with Alcatel SEL AG, D-70435 Stuttgart, Germany (e-mail: asma.ahmed@tuhh.de)
Andreas Diehl is with Alcatel SEL AG, D-70435 Stuttgart, Germany (phone: +49 (0) 711 821 44230, e-mail: andreas.ad.diehl@alcatel.de).

II. Restructuring of Telecommunication Networks

Persistent application data of wireless networks depends on the application location. In particular, mobile (cellular) networks use distributed, decentralized network data nodes to register services. Current mobile network services and databases are distributed all over the network. In Germany the subscriber profiles of GSM networks [11] are separated in more than 40 areas (see Figure 1). Each area consists of the main mobile databases, which are the Home Location Register (HLR) and the Visitor Location Register (VLR). Decentralized subscriber data has deficits in terms of service installation and administration. This circumstance has marked the need of the novel approach of a centralized Next Generation Profile Register (NGPR, refer to Figure 2) [7] [8] [9]. This register may be accessed by all legacy network nodes over gateway functionalities or directly via modern service-oriented architectures. Centralized subscriber data simplifies service integration and billing because of direct access to non-distributed service data and complete subscriber profiles [7].

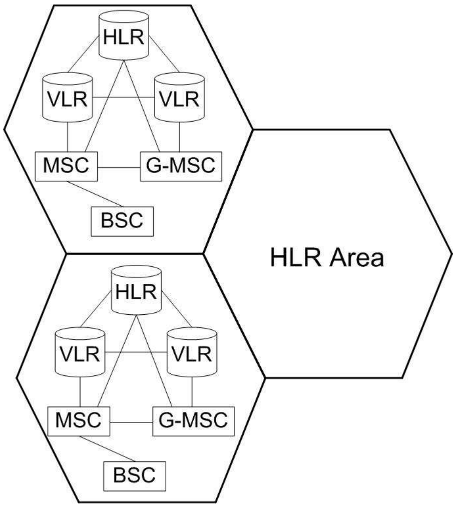


Fig. 1. Distribution of data in GSM networks
BSC: Base Station Controller, **MSC**: Mobile Switching Center,
G-MSC: Gateway-MSC, **VLR**: Visitor Location Register,
HLR: Home Location Register

Additional services may also be supported, e.g. Customer Relationship Management (CRM), Data Mining and Knowledge management.

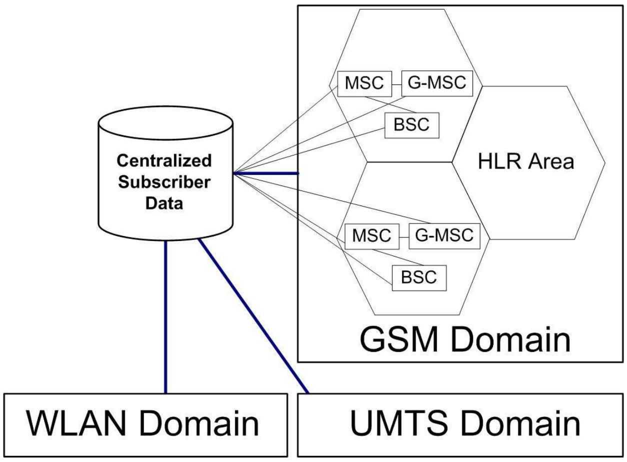


Fig. 2. Future Approach of a Next Generation Profile Register (NGPR)

III. Authentication in wireless networks

Authentication is the process of proving the identity of a certain entity, thus enabling certain rights to a given service. The entity could be a device or a user of a certain service.
Three different authentication methods are considered in the development of the ontology, namely GSM, UMTS and WLAN authentication.

Different methods are used for authentication based on the different technologies used.

A. *Mobile Authentication (GSM / UMTS)*

GSM is the most popular, second-generation system of mobile networks, whereas UMTS is a third generation system of mobile networks. UMTS builds on GSM and is more enhanced in terms of security.

The basic concept behind authentication in both GSM and UMTS networks is a challenge-response mechanism. The mobile device sends out a challenge to the network, represented by the International Mobile Subscriber Identity (IMSI). The network sends out a response based on specified algorithms and the calculation and generation of certain keys. A response is also calculated on the user side after the reception of a certain key from the network. If both responses generated from the user and the network match the authentication procedure is completed and access is granted to the user of the network.

The difference between GSM and UMTS authentication can be summarized as follows:

- UMTS is much more advanced than GSM in terms of security and authentication.
- UMTS uses the Universal Subscriber Identity Model (USIM) card, whereas GSM uses the Subscriber Identity Model (SIM) card.
- UMTS uses and generates more keys for authentication.
- UMTS uses different algorithms to generate the authentication vectors.
- UMTS uses different authentication and key agreement mechanisms.
- UMTS performs mutual authentication. (Both the user and the network are authenticated).
- UMTS provides multimedia services and thus requires different databases for subscriber profiles.

B. *Authentication in WLAN networks*

The main components of a Wireless LAN are the wireless station (e.g. a PC or laptop), the access point, a user database and the Authentication, Authorization and Accounting (AAA) Server.

WLAN Authentication has not been standardized. Hence, there are many different ways of authentication in WLANs, this depends on the methods chosen and deployed for the WLAN connection.

There are basically two methods of authentication in WLAN networks, namely password-based authentication and certificate-based authentication. Several password and certificate-based authentication methods exist. For example, an 802.1x [13] authentication method is based on the Extensible Authentication Protocol (EAP) protocol. Many variants of the EAP protocol [14] referred to as the authentication type exist.
Examples for password-based EAP authentication types are the EAP-Message Digest-5 (EAP-MD5) [12] and Lightweight-EAP (LEAP). Examples for certificate-based EAP authentication are EAP-Transport Layer Security (EAP-TLS), EAP-Tunnelled-TLS (EAP-TTLS), Protected-EAP (PEAP)).
Other variants of the EAP Protocol that act as a bridge between mobile and wireless networks are the EAP-SIM [15] [16] [17] and the EAP-Authentication and Key Agreement (EAP-AKA) [18].

C. *EAP-SIM and EAP-AKA*

EAP-SIM and EAP-AKA (work in progress) are authentication protocols, which are used in GSM and UMTS mobile networks respectively. EAP-SIM is based on the second generation GSM Subscriber Identity Model, whereas EAP-AKA is based on the third generation UMTS Authentication and Key Agreement techniques.

EAP-SIM and EAP-AKA allow users of a wireless network to access the network via the SIM and USIM of the GSM and UMTS networks respectively. This is usually used for billing purposes, so that the user of the network is directly charged according to his/her GSM/UMTS network provider.

The components needed for EAP-SIM and EAP-AKA authentication methods are a hybrid between WLAN networks and GSM/UMTS networks.

The client (e.g. mobile phone, PDA, Laptop) requests access to the network via the SIM/USIM card. Special devices exist for reading the information contained in the SIM/USIM (e.g. USB SIM readers, PC card access or smart card readers)

The client requesting access to a wireless network connects to the network via a wireless access point and the AAA server, which uses the information stored on the SIM/USIM card (IMSI) to access the GSM/UMTS networks through a specific GSM/UMTS gateway. Authentication data is then retrieved and if verified the AAA server grants access to the client.

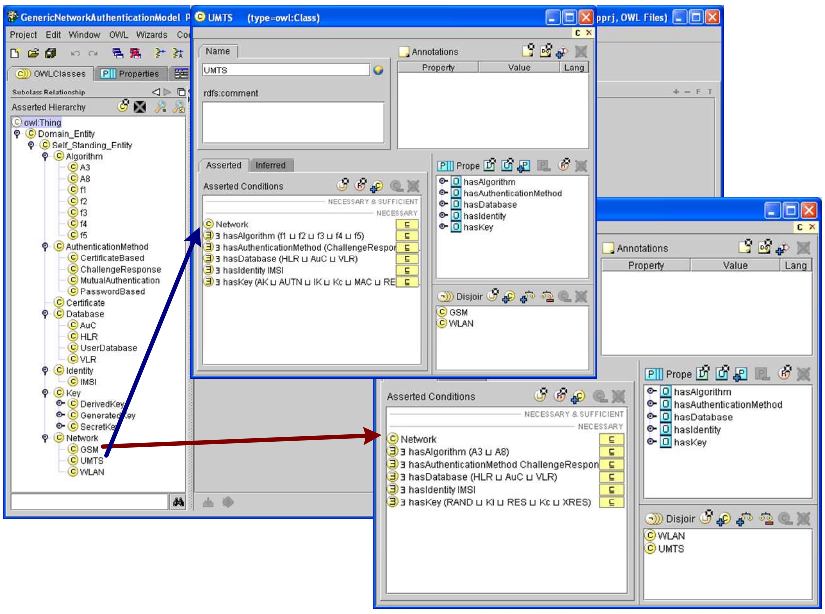
D. *Generic Data Model for wireless Authentication*

In order to build the generic wireless authentication model, it was necessary to analyze the authentication procedures of UMTS, GSM and WLAN networks. After analyzing the network requirements, a list of the different parameters and how they relate to each other was made.

Based on this authentication-data list the first steps in creating the ontology were carried out. A general overview of the network components related to authentication and the main constraints and properties that relate the components to each other were modeled.

Despite the network methods being different in terms of the authentication parameters and the processes and methods used to perform authentication. Common components, parameters and procedures exist between these components.

The ontology's objective is to describe the components and parameters needed for authentication in the afore-mentioned wireless and mobile networks. The ontology works towards illustrating the commonality and differences between the authentication methods. Furthermore, it aims to describe the dependencies, relationships, properties and the restrictions existing between the networks in terms of authentication. The ontology has been partly implemented and further work is currently being performed.



Asserted Conditions (UMTS)

NECESSARY & SUFFICIENT
NECESSARY
Network ⊑
∃ hasAlgorithm (f1 ⊔ f2 ⊔ f3 ⊔ f4 ⊔ f5) ⊑
∃ hasAuthenticationMethod (ChallengeRespor ⊑
∃ hasDatabase (HLR ⊔ AuC ⊔ VLR) ⊑
∃ hasIdentity IMSI ⊑
∃ hasKey (AK ⊔ AUTN ⊔ IK ⊔ Kc ⊔ MAC ⊔ RE ⊑

Asserted Conditions (GSM)

NECESSARY & SUFFICIENT
NECESSARY
Network ⊑
∃ hasAlgorithm (A3 ⊔ A8) ⊑
∃ hasAuthenticationMethod ChallengeRespon ⊑
∃ hasDatabase (HLR ⊔ AuC ⊔ VLR) ⊑
∃ hasIdentity IMSI ⊑
∃ hasKey (RAND ⊔ Ki ⊔ RES ⊔ Kc ⊔ XRES) ⊑

Fig. 3 Protégé view of GSM and UMTS Authentication Data

For the purpose of our example, figure 3 describes some aspects of the GSM and UMTS classes:

- The Network class is made out of three subclasses: GSM, UMTS and WLAN, which represent three different networks.
- The other classes, describe the following:
- Algorithm: contains the algorithms specific to GSM, UMTS and WLAN authentication.
- Authentication Method: specifies the authentication methods used by the networks. For example, UMTS uses a ChallengeResponse and a MutualAuthentication type of authentication.
  - Database: describes the databases used by the networks.
  - Identity: lists the identities used for authentication.
  - Key: provides a list of keys, which are used, generated and derived during the authentication process.
- The following properties were defined for the GSM and UMTS classes; hasAlgorithm, hasAuthenticationMethod, hasDatabase, hasIdentity and hasKey.
- Restrictions on the GSM and UMTS classes are assigned using the different properties created.
- The GSM and UMTS classes contain the same property restrictions for the hasDatabase and hasIdentity properties. GSM and UMTS both use the HLR, VLR and the Authentication Center (AuC) as databases and they both use the IMSI (International Mobile Subscriber Identity) as a subscriber identity.
- The restrictions for GSM and UMTS regarding the hasAlgorithm property are different for both classes. GSM uses the A3 and A8 Algorithms while UMTS uses the f1, f2, f3, f4 and f5 algorithms.
  - The UMTS class uses the ChallengeResponse and MutualAuthentication classes as restrictions for the hasAuthenticationMethod, while GSM only uses the ChallengeResponse class.
  - The UMTS class uses the following subclasses as restrictions for the hasKey property (AK, AUTN, IK, Kc, MAC, RES, XMAC, XRES, RAND, SQN, Ki) while the GSM class only uses the (RAND, Ki, RES, Kc, XRES) subclasses [10].

IV. Conclusion

For wireless telecommunication networks centralized NGPR are a challenging instrument for data integration from different access networks. This paper gives a short introduction into wireless authentication methods and gives an ontology overview of wireless, authentication data of a NGPR. The generic approach unifies different existing authentication data models being used in the most popular wireless access networks. Therefore the integration of authentication methods in other networks or authentication re-usability can be realized. Further work to be carried out is the integration of additional subscriber data and an evaluation of the concept by a concrete implementation of the data model.

References

[1] 3GPP TS 41 series (2005), "GSM only Requirements", Available: March 25 2005, http://www.3gpp.org/ftp/Specs/html-info/41-series.htm, Valbonne; France.

[2] 3GPP TS 42 series (2005), "GSM only Service Aspects (Stage1)", Available: March 25 2005, http://www.3gpp.org/ftp/Specs/html-info/42-series.htm, Valbonne; France.

[3] 3GPP TS 43 series (2005), "GSM only Technical Realization (Stage2)", Available: March 25 2005, http://www.3gpp.org/ftp/Specs/html-info/43-series.htm, Valbonne; France.

[4] 3GPP TS 21series (2005), "3G GSM R99 and later Requirements", Available: March 25 2005, http://www.3gpp.org/ftp/Specs/html-info/21-series.htm, Valbonne, France.

[5] 3GPP TS 22series (2005), "3G GSM R99 and later Service Aspects (Stage1)", Available: March 25 2005, http://www.3gpp.org/ftp/Specs/html-info/22-series.htm, Valbonne, France

[6] 3GPP TS 23series (2005), "3G GSM R99 and later Technical Realization (Stage2)", Available: March 25 2005, http://www.3gpp.org/ftp/Specs/html-info/23-series.htm, Valbonne, France.

[7] A. Diehl, U.Bleimann, W. Fuhrmann, P.Reynolds and S. Rupp, "Service Architecture for an Object-Oriented Next Generation Profile Register", *5th International Network Conference (INC)*, Samos 2005

[8] S. Rupp, G. Siegmund, R. Lopez-Aladros and F. Banet, "Flexinet – A Network Service Architecture", *Journal of the Communications Network*, Jan-March 2004.

[9] S. Rupp, R. Lopez-Aladros, F. Banet and G. Siegmund. (2004/2) "Flexible universal networks - a new approach to telecommunication services", *The 8th World Multi-Conference on Systemics, Cybernetics and Informatics*, Orlando 2004.

[10] UMTS Security V. Niemi & K. Nyberg, John Wiley & Sons Ltd., 2003

[11] GSM Networks: Protocols, Terminology, and Implementation, Gunnar Heine, Artech House Publishers, 1999

[12] HP Development, "Designing a Secure Wireless LAN with the HP-UX AAA RADIUS Server", Available: April 04 2005, http://docs.hp.com/en/WLANs-AAA/WLANs-AAA.pdf

[13] LXE Inc., Wireless security – The New 'Keeping the Bad Guys out of your 802.11 wireless network' 2004 Edition, Available: April 04 2005, http://www.lxe.com/us/pdf/wp_new_security_80211.pdf

[14] IEC, EAP Methods for 802.11 Wireless LAN Security http://www.iec.org/online/tutorials/eap_methods/

[15] Open Systems Consultants, Pty. Ltd., "Radiator EAP-SIM Support", white paper discussing EAP-SIM authentication support for Radiator. For EAP-SIM Module version 1.2, March 22, 2005, Available: June 01 2005 http://whitepapers.zdnet.co.uk/0,39025945,60055226p-39000375q,00.htm

[16] Meetinghouse, "EAP-SIM Authentication Method for Converging Worlds of Mobile Telephony and Wireless LAN" White paper, Available June 01 2005, www.mtghouse.com/EAP_SIM_031405.pdf

[17] IETF, H.Haverinen, Ed., J. Salowey, Ed., "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)", draft-haverinen-pppext-eap-sim-16.txt, Internet Draft, December 21 2004. Available: June 01 2005 http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-16.txt

[18] IETF, J.Arkko, H.Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", draft-arkko-pppext-eap-aka-15.txt, Internet Draft, December 21 2004, Available: June 01 2005 http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-15.txt

Asma Alazeib is currently a Master student in Information and Media Technologies at the Technical University of Hamburg-Harburg (Germany). She is pursuing her final Master Thesis in developing an ontology for wireless authentication using Protégé at the mobile services department of Alcatel SEL AG, Stuttgart (Germany).

Andreas Diehl graduated with a Master degree in Computer Science at the University of Applied Sciences Darmstadt (Germany). Beside his studies he joined Software AG and completed several successful projects as a Software Developer. Since the end of 2003 he has been working for Alcatel SEL in the area of Software Design and System Architecture of Next Generation Mobile Networks in Stuttgart (Germany). In parallel he started his PhD studies at the University of Plymouth (United Kingdom).