An Advanced Authorization Framework for IP-based B3G Systems

Alexis Olivereau, Antonio F. Gómez Skarmeta, Rafael Marin Lopez,
Benjamin Weyl, Pedro Brandão, Parijat Mishra, Christian Hauser.

***Abstract*— Controlled access to resources offered by network operators and service providers is a key component for any commercial deployment of a Beyond-3G (B3G) communication system: complex scenarios involving users accessing advanced multimedia services using heterogeneous network technologies in different administrative domains do require tight access control.**

This paper presents an authorization model that provides secured access control to network-dependent as well as to applicative services. Stemming from a new identity model that not only protects user's privacy but also allows for more powerful services, advanced authorization procedures are defined.

We describe how innovative enhancements to authentication protocols easily and profitably make them usable for the purpose of authorization. A special focus is put on new registration procedures that can be built on top of these improvements in order to provide new security features to the infrastructure (e.g. granular access control rules, generic security model) while offering new security services to the end user (e.g. anonymity, fast attach procedure).

***Index Terms*— Authorization, PANA, EAP, Authentication, AAA, Id Token.**

I. Introduction

Daidalos (Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services) project [1] aims at seamlessly integrating heterogeneous network technologies that allow network operators and service providers to offer new and profitable services (voice, data, multimedia). As a key component of this architecture, a strong emphasis is given to security [2], especially authentication and authorization. Leveraging on a robust identity model, registration procedures ensure that no user will infringe her rights, be it for launching a Denial-of-Service attack against the network infrastructure or for illegitimately accessing a paying service.

This paper focuses on the authorization framework that has been defined in the Daidalos project. Quoting [3], an authorization process is defined as a procedure for granting rights or permissions to a system entity to access a system resource. The system entity in this paper is the user, characterized by the identity she presents to the authenticator. After a brief overview of Daidalos identity model provided in section II, procedures for access control to system resources are considered in the logical order that a user typically encounters them. Authentication for network access is detailed in section III. The subsequent authorization processes for network-dependent services are considered in section IV. Section V deals with generic authorization for interdomain service access. Finally some conclusions are drawn in section VI.

II. Daidalos Identity Model

In the Daidalos world, a given user would have relationships with many different providers and even many relationships with the same provider. As such, the user may find it desirable that: (a) a passive snooper on the network, or a service provider with which the user does not have a direct relationship should not be able to find out the "real" identity of the user; (b) the aforementioned attacker or service provider should not be able to link multiple invocations of a service to the same user without the user's wishes. If one considers these privacy requirements, the need for a flexible identity model (as opposed to a single identity strictly bound to a charging account) clearly arises. The Daidalos identity model is defined as follows:

When the user signs a contract with a network operator or service provider, the identity under which the contract, the list of consumable resources, the respective profiles and access rights for those resources, are defined, is called Registration Identity (RegID). The RegID is unique within the operator's domain and is operator confidential. For the purpose of having different levels of privacy Virtual Identities (VID) are defined. Users can choose under which VID they would like to consume the resource. A VID could be dynamically derived from RegID by hiding, masking or faking part (or even all) of

Manuscript received February 6th, 2005.

A. Olivereau is with Motorola Labs, Paris, France (e-mail: alexis@motorola.com).

A. F. Gómez Skarmeta and R. Marin Lopez are with University of Murcia, Murcia, Spain (e-mail: {skarmeta, rafa}@dif.um.es).

B. Weyl is with BMW Group Research and Technology, Munich, Germany (e-mail: benjamin.weyl@bmw.de).

P. Brandão is with University of Porto, Oporto, Portugal (email: pbrandao@ncc.up.pt).

P. Mishra is with Institute for Infocomm Research, Singapore (email: parijat@i2r.a-star.edu.sg).

C. Hauser is with University of Stuttgart, Stuttgart, Germany (email: hauser@ikr.uni-stuttgart.de).

The work described in this paper is based on results of IST FP6 Integrated Project DAIDALOS. DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

the information/profiles originally specified in RegID. Thus VIDs also contain a set of information (i.e. a profile) for each resource the user may wish to consume using that VID. A VID can be persistent if the user wants to use it repeatedly, otherwise it can also be generated and used for a single session or event, and not re-used. Note that the VID format has been derived from the Network Access Identifier format [15], and looks like a user FQDN.

III. AUTHORIZATION FOR NETWORK ACCESS

Obviously, the first network service that is required by a user is basic network connectivity (the right to send and receive data packets, even with a limited scope, over the network), whose access is granted through a specific network access control procedure. Most specifications for this procedure place it at link layer (e.g. 802.1X port-based authentication [4] for Ethernet or 802.11 links). Recently, a working group has been created at the IETF to develop a protocol above IP (PANA [5]) that will carry authentication messaging independently of the underlying link technology.

A. PANA-based Authorization for Network Access

Daidalos is the first European project to deploy a PANA-based architecture for providing network access control. Next, we will briefly describe this new protocol and its advantages.

PANA (Protocol for carrying Authentication for Network Access [6]) aims at offering a single authentication method at the IP layer, above different link technologies for multi-access and point-to-point links. PANA defines how a PANA Client (PaC) authenticates to a PANA Authentication Agent (PAA), which may rely on an Authentication Server (AS) to perform credentials verification. PANA design supports various types of deployments; PaC is normally placed in the user terminal whereas PAA is by definition to be placed at a 1-IP-hop distance from PaC, typically in a Network Access Server (NAS).

PANA protocol runs between the PaC and the PAA and carries an EAP (Extensible Authentication Protocol [7]) authentication method, using UDP as transport layer protocol. In most cases, PANA authentication involves a distant AAA (Authentication, Authorization and Accounting) server that communicates with the PAA using an AAA protocol. PANA access control procedure then fits into a larger AAA-based access control framework. AAA server with enhanced Auditing and Charging features, as it is defined is Daidalos, is thereafter designed as "A4C server".

Link-layer-agnostic mutual authentication and fast re-authentication are keywords when summarizing what PANA is designed for. PANA does not provide traffic confidentiality by itself. Yet, PANA is able to bootstrap a confidentiality protocol at link (e.g. 802.11i [20]) or IP (e.g. IPsec [19]) layer [8], [9]. The secure tunnel is established between the PaC and the PANA Enforcement Point (EP), which is dynamically configured by the PAA upon successful authentication.

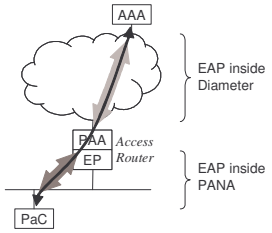

Fig. 1. PANA architecture in Daidalos. PAA and EP are collocated inside the Access Router. End-to-end EAP messages for authentication are carried over EAP between the PaC and the PAA, then over Diameter [21] between the PAA and the AS, which is actually an AAA server.

PANA is able to carry information by using Attribute Value Pairs (AVPs); the base protocol defines the ones required for operation. The protocol supports the definition of new AVPs to contain new values, thus allowing application specific AVPs.

This feature is being used in the Daidalos project to carry authorization information between access networks and users (see sub-section III.B).

Initially, an authentication process is needed to provide the user's device with authorization parameters: ID-token.

The Identity Token (ID-token) is a data entity that contains authorization information related with a particular VID. This ID-token is delivered to the provider to get access to a resource. By using this ID-token, the user does not need to be authenticated again to the resource's owner because it already contains the authorization information needed to access this resource. The format is depicted in Fig. 2.

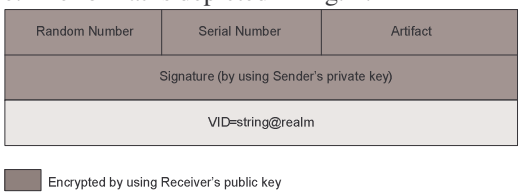

Fig. 2. ID-token internal structure. *Random Number* makes the ID-token different each time it is sent. *Serial Number* helps avoiding replay attacks; its value is maintained by the A4C server. *Artifact* is a reference to SAML assertion [18] related with a particular RegID. *Signature* is a digital signature made over the whole ID-token by using the sender's private key.

This ID-token – which is an authorization token – is only provided when the user has been successfully authenticated by any entity being trusted by the resource owner. The retrieved ID-token is first of all used to register to the network. When the token is already present at the user's device, the authentication phase can be bypassed.

In the authentication phase (see Fig. 3), the ID-token must be delivered from A4C server to the user's device in two steps: first A4C sends the ID-token to AR(Access Router)/PAA after EAP authentication using Diameter then AR/PAA sends the ID-token to Mobile Terminal (MT) using PANA.

New defined AVPs for authorization are used in both steps to transport the ID-token generated by the A4C server. In step 1, ID-token AVP is defined in Diameter EAP application [14]. In step 2, PANA (specifically PANA-Binding-Request) transports this AVP to the MT.

In the registration phase, the user must deliver the ID-token to the network for obtaining access. A similar procedure as described above is employed for transporting the ID-token AVP using also PANA and Diameter. Note, that the PANA message for the registration phase is different if it is sent on the PANA session built on the authentication procedure or not. This is related to PANA's state machine. Fig. 3 shows an example where authentication (using EAP-TLS [12]) and registration phase are executed in the same PANA session.

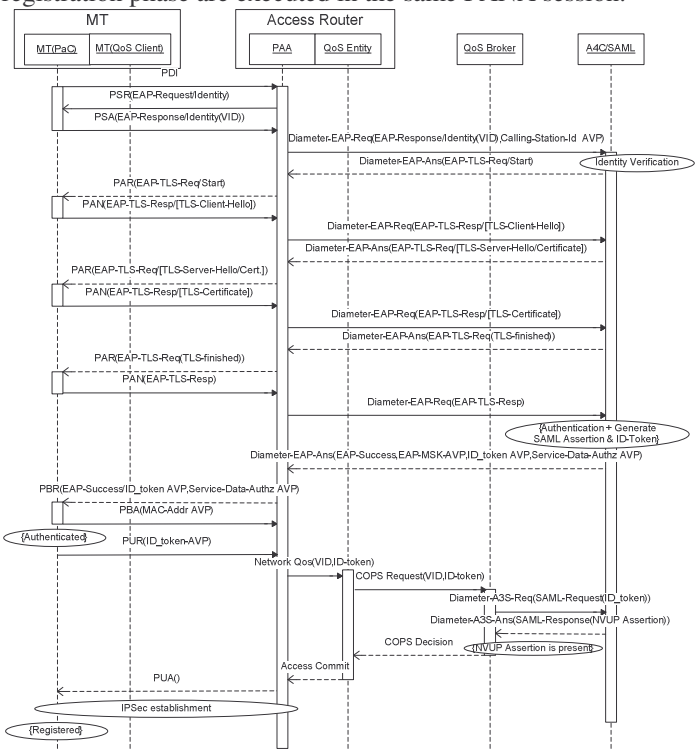

Fig. 3. Authentication and authorization done by PANA.

B. EAP-based Authorization for Network Access

EAP provides a flexible way to authenticate to entities (in particular ad-hoc nodes) because it supports multiple authentication methods. Some EAP methods have the capability to carry generic information apart from authentication information.

The idea of this alternative can be extracted from [11] where it is exposed that some kinds of EAP methods can carry MIPv6 bootstrapping information to MT during EAP-based authentication process. A similar requirement is needed in Daidalos where authorization information (ID-token) must be provided to the user during authentication phase.

During a first approach, we have used PEAPv2 [13] because it provides flexibility to achieve our objectives. It allows the definition of new EAP methods that are encapsulated and carried inside a TLS secure tunnel. This channel is generated during a TLS handshake in the first phase of the protocol. The new EAP method is used to transport the authorization information in the second phase of PEAPv2. Thus, EAP-SAML method is a carrier for ID-token assertions and authorization information.

Note that the PANA protocol is used as EAP lower layer to transport EAP packets from MT to AR. The authentication sequence and ID-token delivery to MT is shown in Fig. 4.

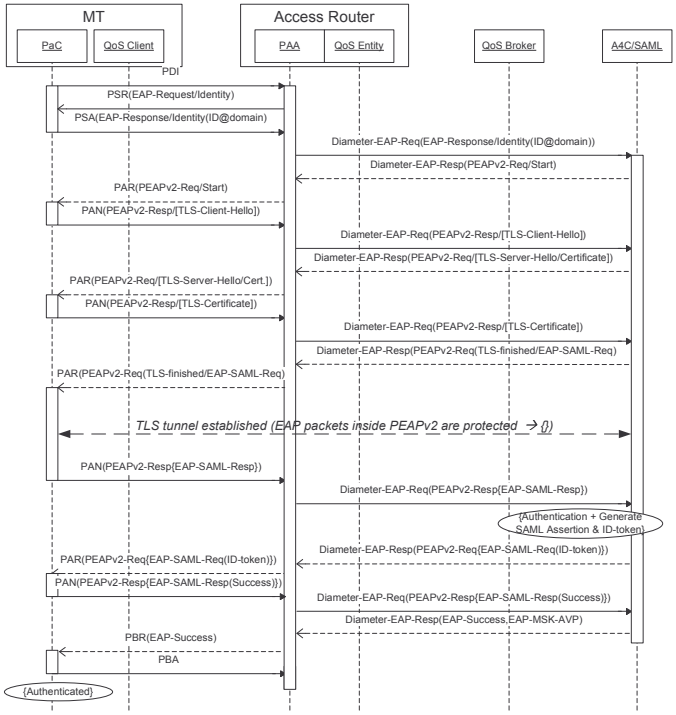

Fig. 4. Authentication phase and ID-token delivery.

Fig. 5 shows the registration process when the user already has an ID-token. As we can see a new PANA session is executed. PEAPv2 TLS tunneled phase 2 is used to deliver the ID-token. In this case only the A4C is authenticated by the MT because the user does not need to be authenticated again as she already owns the ID-token.

In the second phase, A4C requests the ID-token from the user by using the new EAP method (EAP-SAML request/response).

After A4C verifies that the ID-token is correct, it informs the AR/PAA that this user is authorized to access the network. Then AR/PAA requests the QoS Broker to obtain quality of service parameters associated to this user and to know if it is possible to get access. Note that AR has to recover both VID and ID-token to carry out the registration process. However, it cannot access the EAP messages because they are encrypted inside a TLS tunnel. Thus, A4C sends both parameters to AR/PAA by using new Diameter AVPs: VID AVP and ID-token AVP that are added to Diameter EAP Application.

This approach has a clear advantage: access equipment does not need to be modified to support this solution because usually they act as simple EAP messages pass-through. Furthermore, any EAP lower – layer (PANA, IEEE 802.1X) can be used. Additionally, depending on the EAP method used privacy can also be achieved.

However, normally EAP methods that are able to carry additional information consume many round trips and it induces performance degradation. On the contrary, PANA allows a big reduction of roundtrips and the whole process is very much faster in terms of messages than an EAP based

approach. Thus, we are mandating to use PANA in the MT.

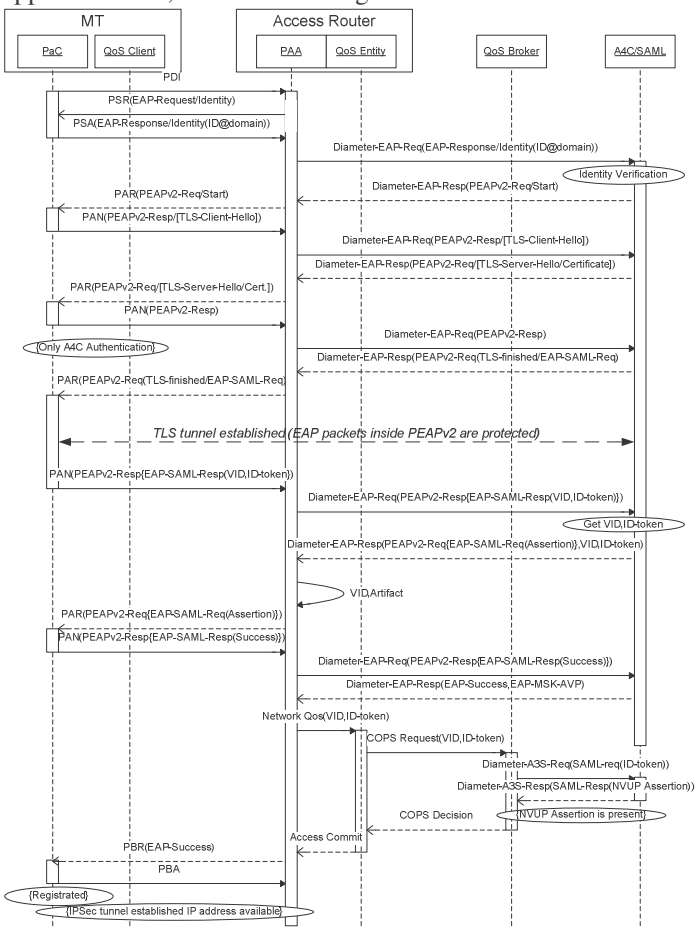

Fig. 5. Registration phase.

IV. Authorization for Network Services

Being operator-driven, Daidalos project considers that network access control is not sufficient to unlock access to all specific network-level features. The use of some optional network features (designated hereafter as "network-dependent services") could be conditioned to certain rights in the user profile (and relevant charging model as well). On the other hand, some of these network-dependent services may require use of software (e.g. specific protocol stack) or hardware (e.g. computing power, memory or bandwidth) resources on some entities in the network. Uncontrolled use of such resources may easily lead to Denial-of-Service attacks against these entities.

For these reasons, Daidalos features specific authorization phases for accessing network-dependent services in addition to the initial authentication/authorization phase that allows for basic network access.

A. Protocol Discussion

In this part, we will justify our choice to use PANA for carrying authorization messages for network-dependent services.

First it is worth giving a brief overview of what these services may consist in. We consider a service may be considered as a network-dependent one if:

- Its functionality is offered at IP level or below;
- Its use may be restricted by the network operator for charging reasons and/or network management reasons, without altering basic network access for the user.

Hence, the following IP features fit into that category: port filtering (allow the user to send/receive traffic to/from specific ports); Quality of Service packet marking (allow the user to mark the packets she sends with specific QoS labels for adequate management at the access router); Mobile IP (allow the user to use Mobile IP); Multicast Receiver Access Control (allow the user to become a member of a multicast group).

Having stated that such services may require an independent authorization phase, the question arises to determine which protocol is the most suitable for carrying that authorization sequence. Here, a subtle difference has to be made between the network-dependent services that actually involve the access router and the ones that do not touch it. For example, port filtering requires that the access router releases some filters once the user has been successfully authorized. On the other hand, Mobile IPv6 does not require setting up rules on the access router; only the Home Agent is affected.

In the case of Mobile IPv6, a specific authorization protocol (possibly based on EAP) can be run directly between the user's device and the home network (the home agent belonging to the home network).

When the access router is affected by the authorization phase though, a mechanism similar to the one involved for network access control has to be featured. That is, the authorization phase must be on either PANA (authorization between the PaC and the PAA) or EAP (authorization between PaC and AAA, with feedback given to AR in the form of an EAP message).

B. PANA-based Example

PANA was historically defined to carry authentication only, with binary authorization results (either access to the network is accepted, or it is refused). After a PANA session had been established between the PaC and the PAA, the only PANA messages that the PAA could have accepted from the PaC were the PANA-Reauthentication and the PANA-Termination ones. Yet, some new PANA messages have been defined recently [6] that allow updating a PANA context in a secure way (taking advantage of the existing PANA Security Association). These new messages are PANA-Update-Request and PANA-Update-Answer, which can be used to carry customized AVPs.

The network-dependent service example we have chosen to depict in this paper concerns multicast receiver access control. In a nutshell, the problem is the following: a multicast group, even if secured through the use of an encryption key, must actively control which members subscribe to this group, so that malicious nodes could not join and thus launch DoS attacks against their local access network [16]. Hence the default behavior for an access router in Daidalos is to silently discard MLD (Multicast Listener Discovery [17]) Report messages as long as the node wishing to receive multicast traffic has not

been authorized for doing so.

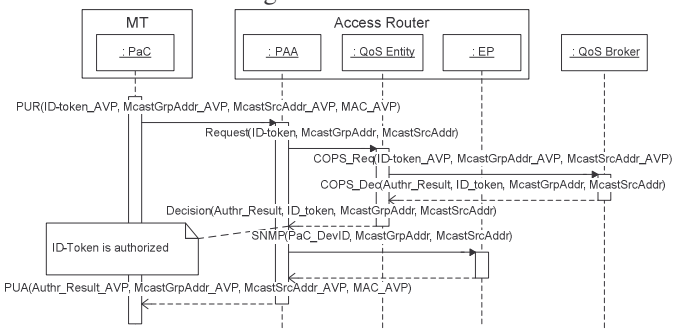

Fig. 6. Multicast receiver access control. PANA Update Request (PUR) and PANA Update Answer (PUA) messages are used to carry respectively authorization request for accessing a multicast group and authorization reply. QoS Broker is consulted by the PAA to determine if enough resources are available and if the node (identified by its ID-token) is authorized to join.

V. INTERDOMAIN SERVICE AUTHORIZATION

Providing an open, standardized and secure solution for distributing personalized services to consumers is a precondition for efficiently introducing new services. Independent Service Provider (SP) and federation concepts arising correspond well with Beyond-3G networking paradigms.

Access-control in this environment must enable a customer's secure service consumption across federated domains. The proposed ID-token approach builds on SAML, which facilitates the secure access greatly, by providing independence from specific authentication mechanisms and the seamless usage of services without being actively confronted with an authentication mechanism, enabling a smooth, practical and enjoyable inter-domain consumption of services [22].

The process flow is described as follows: the ID-token is included within the service request from the MT to the SP, where it can be extracted. The SP sends this token to the responsible A4C.

The A4C decrypts the token, verifies the signatures and maps the ID-token to the corresponding authentication assertion, which has been created during initial authentication, This assertion is used for checking user's authentication session status. Then, a profile-specific attribute and authorization assertion, which is related to the VID, is created and sent to the SP.

When the user is not accessing an SP in its home domain, the same procedure applies from the MT's point of view. However, the foreign A4C cannot access the ID-token, and thus is unable to verify it. It must then request the A4C from the user's home domain for the verification of the ID-token and the generation of the VID-specific authorization assertion. The ID-token has information on which A4C to contact through normal AAA routing. Federation will be based on A4C's interconnection and trust establishment.

VI. CONCLUSION

A solution for providing authorization for network access & services as well as applicative services has been proposed. This approach is based on enhancements to classical authentication-carrying protocols, which allow them to carry anonymous, yet accurately context-related, authorizing material.

Next steps will consist in going further in the development of authorization protocols at the edge of the network. New EAP methods (instead of existing ones), new PANA messages (instead of new AVPs) will have to be defined for that purpose. Obviously, these developments will require parallel improvements in the core network authorization features.

REFERENCES

[1] http://www.ist-daidalos.org

[2] "Security Framework Design Specification", Daidalos (IST-2002-506997) Deliverable, D331, Aug 2004.

[3] R. Shirey, "Internet Security Glossary", IETF RFC2828, May 2000.

[4] "Standard for Local and Metropolitan Area Networks – Port-based Network Access Control", IEEE, December 2004.

[5] Protocol for carrying Authentication for Network Access (pana), http://www.ietf.org/html.charters/pana-charter.html.

[6] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-07 (work in progress), December 2004.

[7] L. Blunk, J. Vollbrecht, , J. Carlson, H. Levkowetz "Extensible Authentication Protocol (EAP)", IETF RFC 3748, June 2004.

[8] P. Jayaraman, R. Lopez, Y. Ohba, M. Parthasarathy, A. Yegin, , "PANA Framework", draft-ietf-pana-framework-03 (work in progress), December 2004

[9] M. Parthasarathy, "PANA Enabling IPsec based Access Control", draft-ietf-pana-ipsec-05 (work in progress), December 2004.

[10] Y. El Mghazli, Y. Ohba, J. Bournelle, "SNMP usage for PAA-2-EP interface", draft-ietf-pana-snmp-02 (work in progress), October 2004.

[11] Giaretta, G., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-02 (work in progress), October 2004.

[12] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", IETF RFC 2716, October 1999.

[13] Josefsson, S., Palekar, A., Simon, D. and G. Zorn, "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-10 (work in progress), October 2004.

[14] Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-08 (work in progress), June 2004.

[15] Aboba, et. al., B., "The Network Access Identifier", draft-ietf-radext-rfc2486bis-03.txt (work in progress), November 2004.

[16] M. Kellil, "Multicast Receiver and Sender Access Control and its Applicability to Mobile IP Environments: A Survey", to be published on 2nd quarter issue 2005 of IEEE CST.

[17] Rolland Vida and al., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[18] Ph. Hallam-Baker, E. Maler (eds.), "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1," OASIS Standard, Version 1.1, September 2nd 2003, http://www.oasis-open.org

[19] S. Kent, R. Atkinson, "Security Architecture for Internet Protocol", IETF RFC 2401, November 1998.

[20] Institute of Electrical and Electronics Engineers, "Supplement to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE 802.11i, July 2004.

[21] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko "Diameter Base Protocol", IETF RFC3588, September 2003.

[22] B. Weyl, H.-J. Vögel, H.-U. Michel: "Integrated Authentication for Telematic Services and Beyond-3G Access Infrastructures using SAML", in Proceedings of IST Mobile & Wireless Communications Summit, pp. 212-217, Lyon., France, June 2004.