2009 Third International Conference on Network and System Security

Trusted Network Access Control in the eduroam federation

Fernando Bernal, Manuel Sánchez, Gabriel López, Antonio F. Gómez-Skarmeta
Department of Information and Communications Engineering
University of Murcia
Murcia, Spain
{*fbernal,manuelsc,gabilm,skarmeta*}*@um.es*

Óscar Cánovas
Department of Computer Engineering
University of Murcia
Murcia, Spain
ocanovas@um.es

***Abstract*—In order to ensure end user devices are healthy enough to gain access to the network, providers are making use of advanced network access control solutions, which propose an evaluation of configuration information (posture) about the device itself before providing access to the network. However, current solutions are focused on intra-domain scenarios, where end users and network belong to the same organization. This work proposes an architecture to provide this trusted network access control in other emerging scenarios: network roaming federations, like eduroam, where the accessed network provider is not where the end user belongs to. The paper describes how authentication and authorization mechanisms for these scenarios can be integrated to provide trusted network access control.**

***Keywords*-network access control, NEA, eduroam, federation**

I. Introduction

Network providers are concerned about how to ensure end user devices, or end points, are healthy enough not only to prevent any security risk to the own providers, but also, to avoid becoming the target of security attacks inside the network. These objectives are driven by advanced network access solutions, also known as advanced Network Access Control (NAC), which have been promoted by different standardization bodies and private companies.

The main objective is to extract the required configuration information (posture attributes) from end user devices to make sure devices are compliant with the network access requirements, established by means of posture policies defined by the network provider. This information covers operating system product and version, installed packages or updated antivirus software.

Different solutions can be found to deploy this scenario. On the one hand, private companies have defined their own solution, like CISCO NAC [4] or Microsoft NAP [9]. They provide robust solutions, but lack a standardized proposal. On the other hand, organizations like the Trusted Computing Group, by means of the Trusted Network Connect Group TNC [13], and the IETF, by means of the Network Endpoint Assessment (NEA) chapter [11], are working on the definition of a standard framework.

Once the end user has been successfully authenticated for network access, i.e. by means of private credentials, providers authenticate the end user device (platform). At this point, providers request posture information to the end user device (they know end user device satisfies posture requirements), before notifying the end user. Only when these processes have been carried out by the provider, the user gains access to the network.

Following this approach, providers authenticating the end users are in charge of both authenticating the user platform and checking the health of devices. This solution is feasible for network providers willing to control the access for their own users to their own network, which is the common case for local internet service providers, where authentication services, network enforcement points and posture decisions entities are located in the same organization. However, new arising scenarios are changing the behavior of end users, and one of the most relevant is the network roaming.

In roaming scenarios, the end users who belong to a home network provider (home domain), where they have defined their user authentication credentials, move to other organization, requesting access to the network (visited domain). Several initiatives, like eduroam [6], deployed in more than thirty countries, or Internet2 SALSA-FWNA [7], are clear examples of them.

In these scenarios, end users authentication is made by an authentication provider located at their home domain (usually by some protected EAP method [2]), while the network enforcement decision is taken by the visited provider, based on the previous authentication decision. In line with the NAC approach, home domains should also authenticate the user platform and recover and process the posture attributes, in order to decide the health of the end user device requesting access. But this implies home domains have to decide on what kind of operating systems, antiviruses or running processes are or are not suitable for an external organization (visited domain), which is not a valid solution.

Beside, posture attributes can not be recovered directly by the visited domain (visited RADIUS server) because these attributes are exchanged over a protected EAP channel established during the end user authentication phase, once the platform has been also authenticated by the home domain.

This problem, which is out of the scope of the current IETF NEA proposal [11], has also been detected by the TNC working group, that recently published a first proposal

978-0-7695-3838-9/09 $26.00 © 2009 IEEE
DOI 10.1109/NSS.2009.47

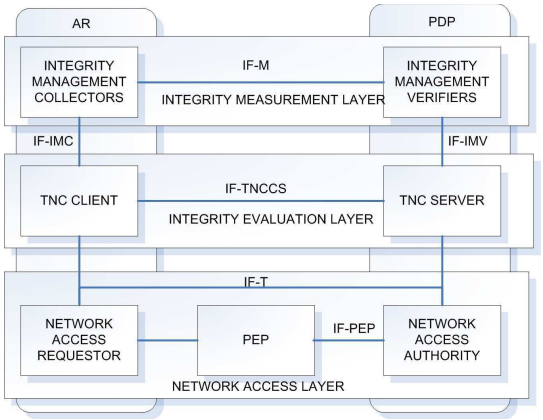

Figure 1. TNC architecture

for federated TNC [16]. That generic proposal is based on some of our previous works.

This paper proposes a solution to deploy trusted network access control mechanisms into roaming scenarios, by means of integration with a novel network authorization proposal for eduroam, defined by the European DAMe project [8]. We present an infrastructure for the management of posture attributes between organizations, and this will allow the integration with user attributes (role, contract, age, etc.) during an authorization phase. Network authorization will be managed by the domains visited by means of an access control framework based on standard technologies such as SAML [3] and XACML [10].

The paper is structured as follows: Section 2 provides an overview of the TNC NAC solution. Section 3 introduces the advanced authorization and access control framework for the eduroam network. Section 4 presents the requirements, architecture and profiles for the proposed solution. Finally, section 5 provides some conclusions and future work.

II. TNC ARCHITECTURE

The main objective of a TNC-based architecture [13] is to provide network providers with a mechanism able to evaluate the health of the end users devices. Through this process, relevant posture information is obtained, and this could be used for authorization purposes.

It defines three main layers, Fig. 1: *Integrity Measurement Layer* collects and verifies information (posture attributes) from a set of security applications; *Integrity Evaluation Layer* exchange posture information between entities; finally, *Network Access Layer* provides network connectivity and supports standard access technologies (i.e. VPN, 802.1X). Each layer defines a set of components:

- *Integrity Management Collectors (IMC)*: checks the system for collecting different posture attributes (i.e. antivirus version, operating system, etc.).
- *TNC Client (TNCC)*: from the end user device, collects integrity measurements provided by the Integrity Measurement Layer and organizes the posture information.
- *Network Access Requestor (NAR)*: end user device element responsible for establishing the network access, normally called supplicant in 802.1X.
- *Integrity Management Verifiers (IMV)*: verifies integrity aspects, by means of the different measurements or attributes received from Integrity Management Collectors. It checks the posture policies.
- *TNC Server*: controls the message flow between Integrity Management Verifiers and Integrity Management Collectors, besides compiling and combining information received from IMVs into an overall *Action-Recommendation* to be used by NAA.
- *Network Access Authority (NAA)*: located in the RADIUS server, enforces, based on the decisions received from the TNC Server, whether a particular NAR must be enabled to gain access to the network.

When the end user attempts to gain access, the Policy Enforcement Point (PEP), usually a Network Access Point (NAP), notifies the NAA, and the authentication process starts, usually by means of some EAP method. After the end user has been successfully authenticated the TNC process starts, the authentication of the end user device (platform) is required, and it is usually made by Attestation Identity Key (AIK) credentials. It is worth noting that platform authentication is completely transparent to the end user.

Afterwards, both TNCC and TNCS indicate to IMCs and IMVs a new connection attempt. At this point, an integrity check handshake starts, using a new EAP method (EAP-TNC) to transport the IF-TNCCS messages between end user and provider. During this handshake, posture attributes are collected by the corresponding IMCs. Currently, two main protocols have been defined for attribute exchanging: IF-TNCCS-SOH (Trusted Network Connect Client-Server-Statement of Health) [15] (based on TLV) and IF-TNCSS [14] (based on XML). IF-TNCCS-SOH only supports a single round trip for one 4KB packet, while IF-TNCCS supports several round trips without size restriction.

It is important to note that the EAP-TNC channel is established between the end user device and the authentication server, so intermediate servers (like intermediate RADIUS servers) can not directly manipulate posture attributes.

When the integrity check handshake finishes, an *Action-Recommendation* response is sent to TNCS from each IMV. This response can be positive or negative, depending on each IMV's evaluation. TNCS collects all the IMVs *Action-Recommendation* and notifies the NAA. At this point, the NAA sends the final network access decision to the PEP.

III. DAME

DAMe [1], deployed as part of the TERENA GN2-JRA5 working group, aims to define a unified authentication and

authorization architecture for federated services hosted in the eduroam network [6], which can range from network access control to high-level applications, like Web or Grid services.

eduroam is a RADIUS-based roaming network, which allows an end user from domain A to gain network connection in domain B (with A and B collected to eduroam), but making use of their private authentication credentials defined in A. This authentication process is usually based on an EAP-TLS method, like PEAP, in order to achieve the authentication process.

DAMe extends this RADIUS-based infrastructure in order to include authorization mechanisms [8], making use of authentication tokens and a generic authorization infrastructure like eduGAIN [5]. DAMe provides organizations with the tools to be able to take access control decisions not only based on the end user identity, but also taking into account additional information, in the form of user attributes, like age, contract, role, etc. In this scenario, as before, the authentication process is performed by the home domain, but the final authorization process is made by the visited one, taking into account those user attributes, and making use of an advanced access control policy.

The proposed architecture in DAMe is based on two parallel infrastructures. First, the authentication infrastructure is based on eduroam, therefore each organization makes use of a RADIUS server connected to the eduroam hierarchy. Second, the authorization infrastructure is based on eduGAIN, so each organization is connected by means of a BE (Bridging Element), which provides the required interfaces for authorization mechanisms, in this case, for requesting and providing end user attributes. The visited domain provides network access to roaming users by means of a NAP (Network Access Point) and needs a PDP (Policy Decision Point) to take authorization decisions based on the end user attributes. Finally, the home domain manages all the information associated with their users by means of an IdP (Identity Provider).

A more detailed analysis and performance evaluation of this work can be found in [12].

IV. Architecture Proposal

This section describes our approach for posture assessment in eduroam.

A. Requirements

This section enumerates the set of requirements for the proposed scenario:

- *Platform authentication*. It is necessary to make sure that the end user device guarantees a minimum set of security measures. Platform authentication is required, and it is done at the home RADIUS server.
- *Secure attribute exchange*. Requesting and responding posture and end user attributes must be made in a secure communication channel to avoid an attacker obtaining critical information. It implies intermediate RADIUS servers can not manipulate posture attributes.
- *Access control decisions in visited domain*. For roaming scenarios, final network access decisions must be made in visited domains, since end users must be governed by the visited domain's access policies.
- *Attribute agnostic*. The proposed solution must be generic and extensible for any kind of posture and end user attributes.
- *Standard and less intrusive solution*. The adopted solution must be the least intrusive for the end user and organizations.
- *Intra and inter-domain solution*. Proposed solutions must be valid for either roaming or local end users.

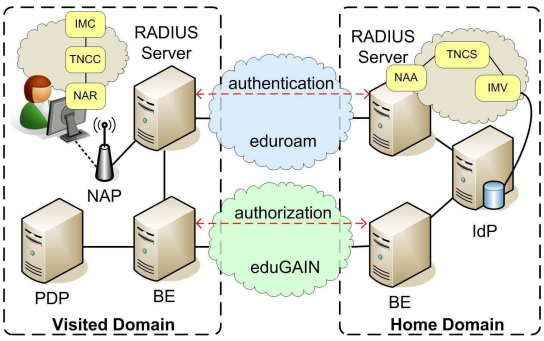

Figure 2. New components in the architecture

B. Proposed architecture

As depicted in Fig. 2, the proposed architecture involves two domains, end user home domain and the visited domain. Home domain represents the organization where the user has their credentials and specific user attributes (i.e. age, contract, role,...), managed by Identity Provider.

In general, home domain will collect all posture attributes during the authentication phase. In line with the DAMe approach, for local and remote users, these attributes will be locally stored, and will be further required during the authorization phase, optionally together with the end user attributes. In this way, the visited RADIUS server, once it is aware the end user is successfully authenticated, and before notifying the user, will launch the authorization process, and will recover all the posture and end user attributes. These attributes will then be combined to get an authorization decision statement from the PDP indicating if the access is denied or granted.

End users have to follow the DAMe requirements: a network supplicant to manage authentication tokens. Besides, they have to run the TNC components described: Integrity Management Collectors, TNC Client, and Network Access Requestor (integrated in supplicant). No additional modifications are required on the user side.

Fig. 2 shows the proposed architecture. When the end

users try to get access to the network, and they are successfully authenticated following the eduroam architecture, before to notify them, then the NAA invokes the TNCS and IMV components. Here, IMV behavior is to store posture attributes locally in the identity provider database, and to return a positive *Action-Recommendation* to the TNCS. In this case, home domain is aware that posture attributes will be evaluated by the visited domain, and there will be further retrieval during the authorization phase. Note that *Action-Recommendation* could be removed from IMVs whenever it ensures that the TNCS provides NAA with a positive recommendation.

It is worth noting that, during transitions phases, different TNCS and IMV components can be used, following the TNC architecture, to distinguish between local and remote users. NAA could decide user connection location by means of the incoming *Access-Request* RADIUS message.

V. Trusted network access control profiles

This section describes in detail the end user authentication and authorization profiles.

A. User Authentication

An end user, belonging to a home domain, wants to gain network access in a visited domain belonging to the same roaming federation, Fig. 3. In eduroam, access control is carried out following the 802.1X standard, that is, the end user is associated to an access point (AP), which contacts its local RADIUS server in order to authenticate the end user. But when the local RADIUS server identifies that the end user belongs to a different domain (based, for example, on the end user identity), the authentication request is forwarded, through the RADIUS hierarchy to the home domain. The authentication process is based on a tunneled EAP Method, EAP-TTLS or EAP-PEAP, because these methods provide a protected channel. At this point, end user identity is authenticated and the usual authentication process in eduroam is extended in order to support end user device authorization by means of the TNC architecture.

Once the end user identity is verified, a connection attempt is notified both on the user side and server side by the TNC components (NAA, NAR), and the platform credentials authentication is performed (i.e. AIK credentials) through TNCC and TNCS. Note that the platform authentication is required by TNC and it is totally transparent to the end user since it is internally performed by the TNC components.

Next, during the Integrity Check Handshake, TNCC and TNCS exchange posture attributes, and IMV is notified in order to store them in the identity provider database. End user identity is used as identifier. In this case, the IMV *Action-Recommendation* and *Evaluation Result* must be always positive.

The Integrity Check Handshake can take several round trips to collect all device data. For this solution, we have deployed the IF-TNCCS interface based on XML because there is no size limit for attributes and because several exchanges could be made. As described above, these messages are transported over EAP-TNC, which are encapsulated into the protected PEAP channel.

Following the DAMe approach, and once the information exchange has finished, an SSO token is built by the Identity Provider (through the local BE), which proves the user has been successfully authenticated. It is then sent back to the user through the PEAP channel. For privacy protection, the generated SSO token contains a *handle* instead of the user identity. This *handle* is also sent back to the visited RADIUS server in a RADIUS attribute with the *Access-Accept* message. As described before, the use of this SSO token is out of the scope of this work and next we focus on the use of the *handle*. Then, the visited RADIUS server can launch the authorization phase before forwarding the *Access-Accept* message to the end user.

B. User and posture authorization

When the visited RADIUS server receives the authentication answer from the home RADIUS server, the *handle* is extracted from the received message and the authorization process starts, Fig. 4. First, following the DAMe authorization architecture for eduroam, the visited RADIUS server asks the local BE for an authorization decision and, if required, specific network parameters that have to be applied to set up the end user connection [8].

The BE is now in charge of recovering all the attributes from the end user home domain, and has to request them from the home BE, which acts as a gateway to provide a generic interface to any kind of identity management solutions provided by the home domain. The location of home BEs is done by asking a Metadata Server element (MDS), defined by the federation.

Once located, the visited BE sends an attribute query message, based on the eduGAIN protocol (SAML-based) to the home BE, using the *handle* for end user identification. Now, using the locally deployed identity management solution (Shibboleth, OpenId, PAPI, etc.) the home BE collects all the required attributes, which include the own end user and posture attributes, stored during the authentication phase. This set of attributes is sent back to the visited BE. Note that attribute query includes the *handle*, although the posture attributes were linked to the end user identity. This can be done because the identity provider knows the match between the *handle* and end user identity.

It is important to note that the visited domain needs to distinguish between user and posture attributes. Each set of attributes could be returned in both an independent *SAMLAttributeStatement* or in a combined one. In any case, attribute identification, for example by means of a *namespace* property, must be used.

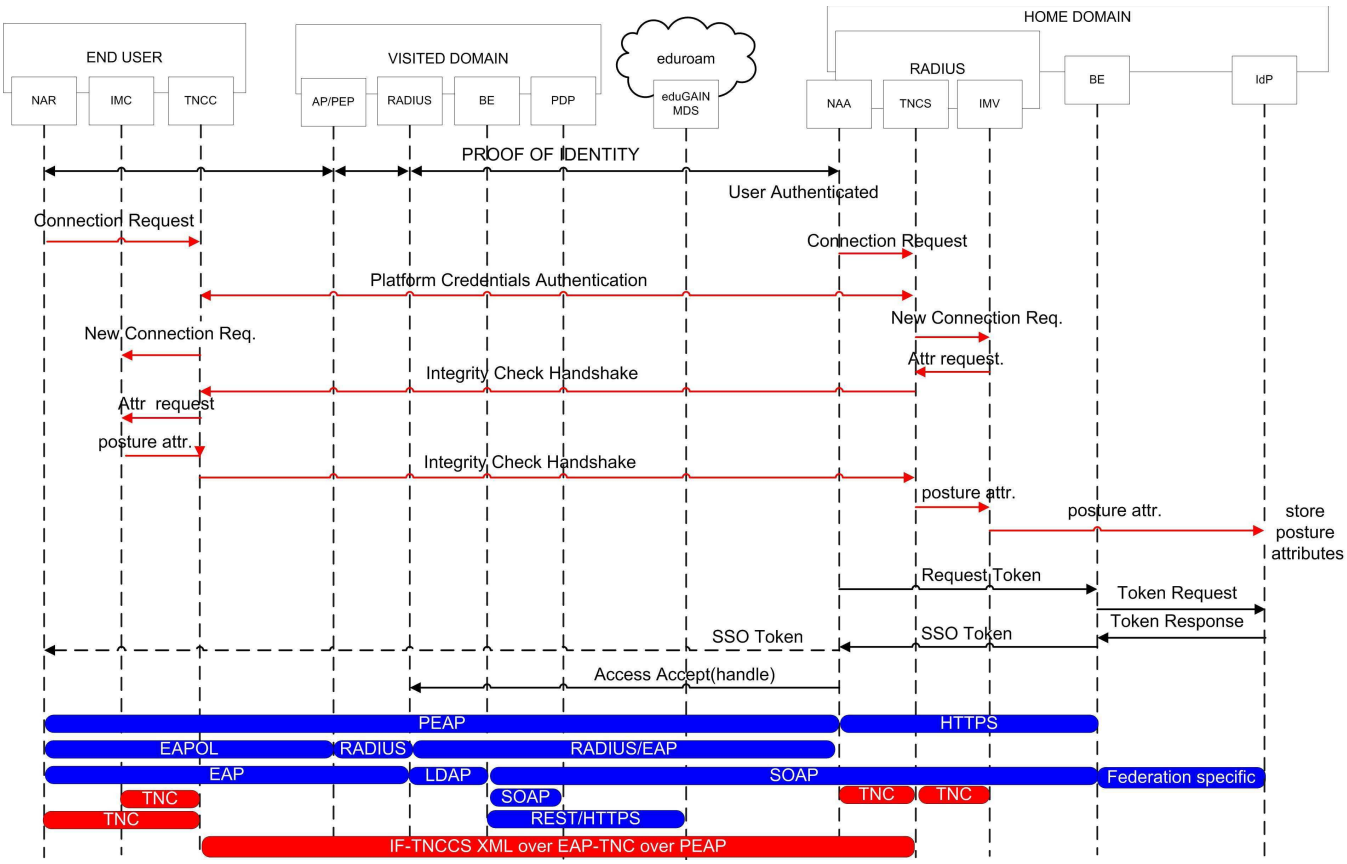

Figure 3. Authentication profile

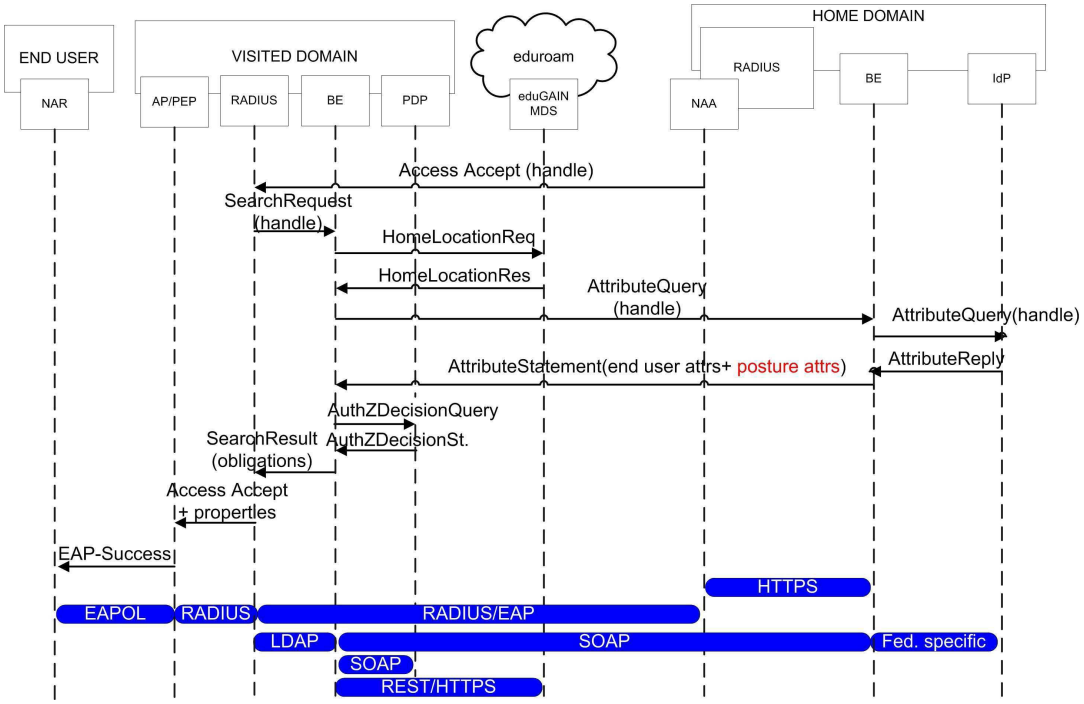

Figure 4. Authorization profile

When attributes arrive, the BE visited queries the PDP in order to obtain a final authorization decision. In line with the DAMe proposal, this query is based on SAML, and is made by means of the *SAMLAuthorizationDecisionQuery/Statment* sentences. This query includes the attribute statements as evidences. The PDP will now check if both, the end user and posture attributes are valid inside the visited domain, based on the access control policies. These policies are based on XACML and they are out of the scope of this paper.

VI. Conclusions

Taking advantage of eduroam, and the extension for end user authorization, this study describes how posture attributes, which concern network providers, can be used in conjunction with the authorization process. This will allow network providers to ensure not only if users are successfully authenticated in their home domains, or if they have the right attributes like contract, entitlement, etc, but also, if they are healthy enough to access the network, and everything is controlled by policies located in the visited domain. The solution proposed makes use of the TNC architecture, and this is extended, in line with the standard interfaces, in order to allow the management of local and remote users.

As a statement of direction we are working on trusted network access control architectures for cross-layer scenarios, and the standardization of posture policies. Additionally, based on the testbed described in [12] we plan to analyze the performance implications of this approach.

Acknowledgment

This work is dedicated to the memory of Manuel Sánchez Cuenca who, before his premature passing, contributed towards the development of the concepts articulated within this paper.

This work has been partially funded by SWIFT (FP7 project, 215832) and CENIT-Segur@. Thanks to the Funding Program for Research Groups of Excellence (04552/GERM/06) granted by Fundación Séneca. This work has been also jointly supported by the Spanish MEC and European Commission FEDER funds (Consolider Ingenio-2010 CSD2006-00046 and TIN2006-15516-C04-03).

References

[1] DAMe project home page, 2009. http://dame.inf.um.es.

[2] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). The Internet Engineering Task Force (IETF) - Network Working Group, June 2004. Request For Comments (RFC) 3748.

[3] S. Cantor, J. Kemp, R. Philpott, and E. Maler (Eds.). Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0, March 2005. OASIS Standard.

[4] Cisco. Cisco's Network Admission Control Main Web Site, 2009. http://www.cisco.com/go/nac.

[5] D.R. Lopez et al. Deliverable DJ5.2.2,2: GÉANT2 Authorisation and Authentication Infrastructure (AAI) Architecture - second edition. GN2 JRA5 (GÉANT 2), April 2007.

[6] K. Wierenga et al. DJ5.1.4: Inter-NREN Roaming Architecture. Description and Development Items. GN2 JRA5 (GÉANT 2), September 2006. Project Deliverable.

[7] Internet2. SALSA-FWNA (Federated Wireless NetAuth), March 2009. http://security.internet2.edu/fwna.

[8] G. López, O. Cánovas, A.F. Gómez-Skarmeta, and M. Sánchez. "A proposal for extending the *eduroam* infrastructure with authorization mechanisms". Computer Standards & Interfaces. Volume 30, Issue 6, August 2008, Pages:418-423, doi:10.1016/j.csi.2008.03.010

[9] Microsoft. Network Access Protection Main Web Site, 2009. http://www.microsoft.com/nap.

[10] OASIS. eXtensible Access Control Markup Language (XACML) Version 2.0, 2005. OASIS Standard.

[11] P. Sangster, H. Khosravi, M. Mani, K. Narayan, and J. Tardo. Network Endpoint Assessment (NEA): Overview and Requirements. IETF - Network Working Group, June 2008. Request For Comments (RFC) 5209.

[12] M. Sánchez, G. López, O. Cánovas, and A.F. Gómez-Skarmeta. "Performance analysis of a cross-layer SSO mechanism for a roaming infrastructure". Journal of Network and Computer Applications. Volume 32, Issue 4, July 2009, Pages 808-823, doi:10.1016/j.jnca.2009.02.004.

[13] Trusted Computing Group. TCG Trusted Network Connect TNC Architecture for Interoperability. Version 1.3, April 2008.

[14] Trusted Computing Group. Trusted Network Connect TNC IF-TNCCS. Version 1.1, February 2007. https://www.trustedcomputinggroup.org/groups/network/.

[15] Trusted Computing Group. Trusted Network Connect TNC IF-TNCCS: Protocol Bindings for SoH. Version 1.0, May 2007. https://www.trustedcomputinggroup.org/groups/network/.

[16] Trusted Computing Group. Federated TNC. Specification Version 1.0. Revision 26, May 2009.