Computer Standards & Interfaces 30 (2008) 418–423

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

A proposal for extending the *eduroam* infrastructure with authorization mechanisms[☆]

Gabriel López [a,*], Óscar Cánovas [b], Antonio F. Gómez-Skarmeta [a], Manuel Sánchez [a]

[a] Department of Information and Communications Engineering, University of Murcia, 30100, Spain
[b] Department of Computer Engineering, University of Murcia, 30100, Spain

ARTICLE INFO

Available online 8 March 2008

Keywords:
NAS-SAML
eduroam
eduGAIN
Authorization
AAA

ABSTRACT

Identity federations are emerging in recent years in order to make easier the deployment of resource sharing environments among organizations. One common feature of those environments is the use of access control mechanisms based on the user identity. However, most of those federations have realized that user identity is not enough to offer more grained access-control and value-added services. Therefore, additional information, such as user attributes should be taken into account. This paper presents how one of those real and widely spread identity federations, *eduroam*, has been extended in order to make use of user attributes and to adopt authorization decisions during the access control process.

1. Introduction

Many aspects of federated approaches to resource sharing, such as user authentication, have been addressed by several projects, as for instance Shibboleth [4], PAPI [12] or Liberty Alliance [2]. However, other aspects generally related with integral identity management still need to be addressed, especially those related to user authorization. Authorization is a critical feature in this environment because when an institution offers its resources to the users belonging to other institutions, it needs to be sure that only allowed users are able to perform the set of allowed actions in each resource.

TERENA Mobility Task Force [18] provided a forum for exchanging experiences and knowledge about the different roaming development activities in the European Union regarding those topics. This working group defined an inter-NREN roaming architecture, called *eduroam* [19], based on AAA servers (RADIUS [16]) and the 802.1X [8] standard. Mainly, *eduroam* allows users of participating institutions to access the Internet at other participants using their home institution's credentials.

The DAMe (Deploying Authorization Mechanisms for federated services in the *eduroam* architecture) [6] project was launched with the main objective of defining a unified authentication and authorization system for federated services hosted in the *eduroam* network. It allows the exchange of additional information (credentials) about the users that might be used to provide a finer-grain access control process. Those federated services can range from network access control to distributed services like Grid Computing.

eduroam already defines how the authentication process is managed inside a federation. Therefore, one of the objectives of DAMe is to define how the authorization process will be included in this infrastructure. For that purpose, this work presents how *eduroam* can be extended with two existing proposals: the NAS-SAML infrastructure [10] and eduGAIN [15]. On one hand, NAS-SAML is a network access control approach based on the AAA architecture and authorization attributes, the SAML (Security Assertion Markup Language) [13] and the XACML (eXtensible Access Control Markup Language) [1] standards. On the other hand, the main goal of eduGAIN is to build an interoperable authentication and authorization infrastructure to interconnect different existing federations.

The rest of this paper is structured as follows. Sections 2, 3 and 4 provide an overview of the *eduroam* service, the eduGAIN infrastructure and the NAS-SAML service respectively. Section 5 points out the set of requirements derived from the integration of those systems, and Section 6 describes the proposed architecture. Section 7 describes some related work that has informed our work and, finally, we conclude the paper with our remarks and some future directions.

2. The *eduroam* service

eduroam (Educational Roaming) is an inter-institutional roaming service based on the 802.1X architecture and a hierarchical RADIUS-based infrastructure. This initiative allows users of participating institutions to access the Internet at other participants' institutions using their home institution's credentials, with a minimal administrative overhead.

The top level server of the RADIUS hierarchy is provided by TERENA, and all the National Research and Educational Networks (NRENs) belonging to the *eduroam* infrastructure are connected to the TERENA one. Finally, each institution willing to join *eduroam* connects its own RADIUS server to the national server of its NREN.

Fig. 1 depicts a user from Home Institution, who wants to get access to the wireless network in Remote Institution, both belonging to *eduroam*. In this situation, the user associates with the wireless

[☆] This work has been partially funded by Daidalos FP6-IP-506997 and DAMe. Thanks also to the Funding Program for Research Groups of Excellence with code 04552/GERM/06 granted by the Fundación Séneca.

[*] Corresponding author. Tel.: +34 968398504; fax: +34 968364151.

0920-5489/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.03.010

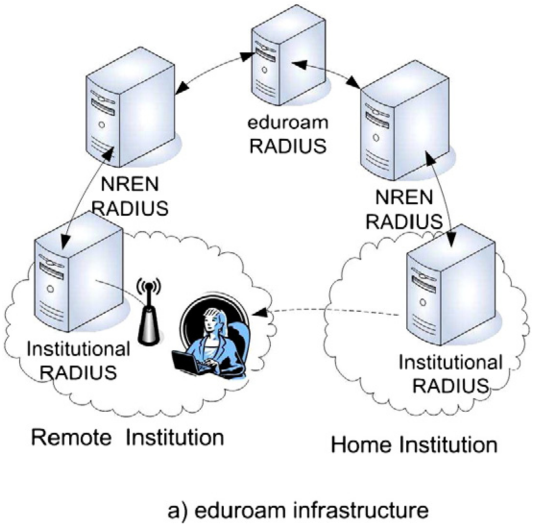


Fig. 1. *eduroam* infrastructure.

access point (AP), through 802.1X, which contacts its local RADIUS server in order to authenticate the user. Once this server identifies that the user belongs to a different domain, based on the user identifier for example, the authent1ication request is forwarded through the RADIUS hierarchy until the server in the user's home institution is reached. Then, the user is authenticated and the response is routed back to Remote Institution, where the AP enables the requested connection.

This proposal makes use of EAP (Extensible Authentication Protocol) [3] for authentication purposes because it allows different authentication mechanisms, such as login and password (EAP-MD5), or digital certificates (EAP-TLS), depending on the required security level.

However, the deployed *eduroam* infrastructure is only useful for user authentication. Thus, remote institutions cannot provide different services for a particular user, taking into account additional information such as user attributes defined in his home institution, which is the main objective of this work.

3. An authentication and authorization infrastructure: eduGAIN

The main goal of eduGAIN is to build an interoperable authentication and authorization infrastructure to interconnect existing federations. In this way, eduGAIN will be responsible for finding the federation where a roaming user belongs, for translating the messages between the internal protocols of the federation and eduGAIN and vice versa, and guarantying trust among the participating institutions. Fig. 2 shows the eduGAIN infrastructure.

The available set of services is included in the MetaData Service (MDS), and a confederation-aware element called Bridging Element (BE) is responsible for connecting the different federations to eduGAIN. Metadata, published by means of the MDS, include information for locating the authentication and authorization points of the federation. In this way, the home federation of a roaming user is located by the remote BE, which obtains the information published in the MDS. The appropriate authentication and authorization requests are then translated and routed by the remote BE to the user's home institution.

The way that the authentication and authorization processes are carried out in eduGAIN is defined by different profiles. Currently, a profile compatible with Shibboleth, called Web SSO, and another one that does not require human intervention, called Automated Client, are defined.

4. NAS-SAML: an architecture for network access control

NAS-SAML [10] is a network access control approach based on authorization attributes and on a configurable authorization system. The proposal is based on the SAML and the XACML standards, which are used for expressing access-control policies based on attributes, authorization statements and authorization protocols. Authorization is based on the definition of access-control policies, including the sets of users pertaining to different subject domains which can be assigned to different attributes in order to gain access to the network of a service provider. The starting point is a network scenario based on the 802.1X standard and the AAA architecture.

In NAS-SAML, every end user belongs to a home institution, where he was given a set of attributes or properties. When the user requests a network connection in a particular institution (home or remote), the request is obtained by the AAA server and, after being authenticated using the corresponding authentication method based on EAP, it makes a query to obtain the attributes related to the user from an authority responsible for managing them. Alternatively, the user can himself present his attributes instead of letting the AAA server recover them. Finally, the AAA server sends an authorization query to a Policy Decision Point (PDP), and that element provides an answer indicating whether the attributes satisfy the resource access policy. That policy can also establish the set of obligations derived from that decision

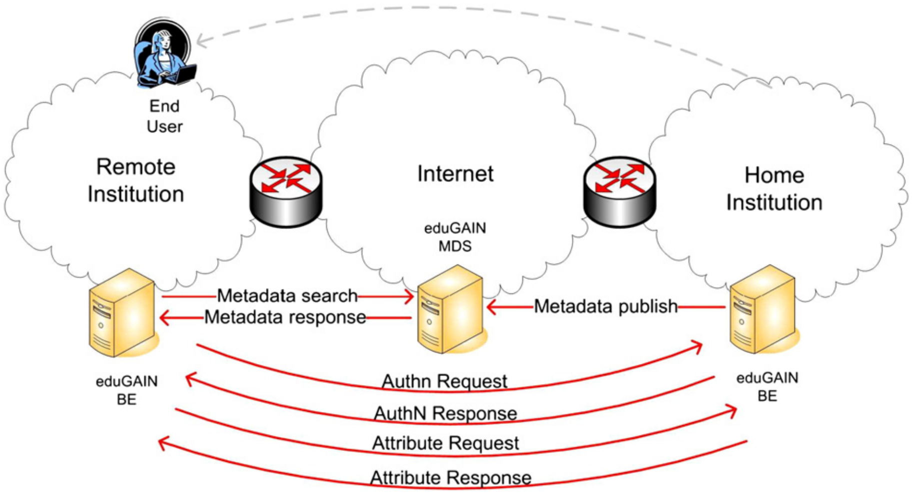


Fig. 2. eduGAIN architecture.

(QoS properties, security options, etc.). This general scheme works both in single and inter-domain scenarios, and uses both push and pull-based communications.

NAS-SAML has been also integrated with other authorization systems, such as PERMIS [11], and some additional prototypes have been defined also for Grid Computing [17]. Moreover, since it is based on SAML, it can be easily integrated with other authentication solutions, such as Shibboleth.

5. Analysis of requirements

In order to integrate authorization mechanisms in *eduroam*, several considerations have to be taken into account.

First, we need a way to recover some user attributes from his home institution. It implies the definition of an authority able to accept requests for those attributes and to decide which ones can be or not revealed to the requesting institution. Usually, this authority depends on the authentication and authorization infrastructure deployed in the home institution. For example, it could be the Identity Provider module defined by Shibboleth, the Authentication Service provided by PAPI, or the Attribute Authority defined by NAS-SAML.

The second requirement establishes that an authorization decision module is required in order to specify which network properties will be enforced. It implies the integration of a Policy Decision Point (PDP) in the remote institution, which takes the final decision about the network access based on the access-control policies. NAS-SAML already provides the definition of this module and defines the required policies by means of the XACML standard.

Finally, the third requirement establishes the need for a communication mechanism able to support the exchange of those authorization credentials inside the federation or even between different federations. It is solved by the integration of the eduGAIN infrastructure in order to get in touch different institutions. As previously described, eduGAIN defines the entities, Bridging Elements (BE), in charge of establishing the communication between federations and institutions. BE offers a well-defined and standard way to obtain authentication, authorization and decision statements in a transparent way to the institution's internal components.

Taking into account these requirements this work proposes an architecture able to provide *eduroam* with the management of user attributes among institutions. This proposal is described below.

6. Proposed architecture

As described in Section 1, the *eduroam* network is mainly composed by a RADIUS hierarchy of authentication servers deployed in each institution. The integration of authorization mechanisms during the network access requires new functional elements in order to fulfill the set of requirements presented in Section 5. However, we have to take into account that *eduroam* is an already deployed network, that is, hundreds of institutions are using it. Therefore it is necessary to introduce changes gradually, maintaining backward compatibility and allowing institutions to introduce the new functionality step-by-step.

The proposed architecture defines the authorization process as a new step after the authentication phase. That is, once the user is authenticated through the *eduroam* network, the authorization phase is triggered by the remote institution. It is worth noting that, with some minimal changes, the *eduroam* authentication phase also needs to be extended.

Following the *eduroam* nomenclature, we define the *Home Institution* (*HI*), where the mobile users belongs to. It is responsible for performing the authentication process and, for authorization purposes, when other institutions request information about users, it must release only the appropriate attributes following a specific policy. We also define the *Remote Institution* (*RI*), where the roaming user is trying to access to the network. It has to determine the properties related to the network connection of the visiting users, according to some specific attributes.

Fig. 3 shows this architecture and the required elements:

- *RADIUS server in RI*: In *eduroam*, it receives authentication requests from the access point (802.1X). When the user belongs to the visited organization the request is processed locally. Otherwise, the request will be forwarded to the appropriate home RADIUS server. As part of the proposal presented in this paper, the RADIUS server must be extended to support the authorization phase in order to request authorization decisions based on the user attributes, once the user is authenticated. In order to provide a common framework, the authorization phase will be performed through the eduGAIN infrastructure.
- *RADIUS server in HI*: In *eduroam*, this server receives authentication requests from remote domains, including user authentication credentials that are validated locally. For authorization purposes, it has to be extended to query, once the user has been authenticated, to the

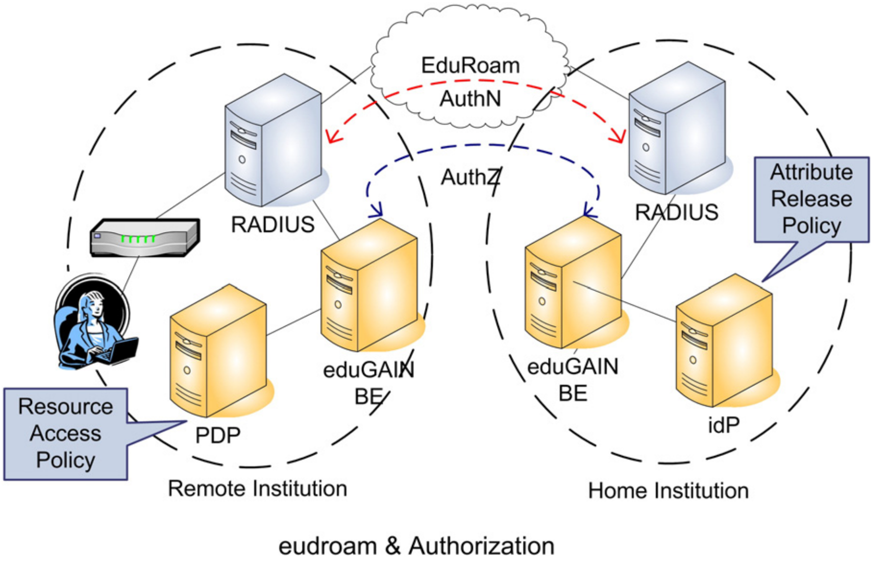


Fig. 3. Proposed architecture.

Identity Provider (*IdP*) for an authentication statement. In this case, the IdP acts as a central point for both authentication and authorization purposes. Together with the authentication statement, pointing out whether the user is authenticated or not, the RADIUS server will receive a handle [7], which is forwarded to RI, and then, if required, used afterward by the remote RADIUS server to request the user attributes credentials. Finally, as described in Section 5, IdP are institution dependent, so in order to provide a common interface between the RADIUS server and the IdP, the communication is made by means of the eduGAIN infrastructure (BE).

- *BE in HI*. Following the eduGAIN architecture, BEs are common points to request authentications and authorizations statements. During the authentication phase, as previously described, we propose to use this element in HI to provide a common interface between the RADIUS server and the local IdP, in order to make IdP specific details transparent to the server. Taking advantage of the already defined BE functionality, this element will be extended in order to generate and manage the authentication handle described above. During the authorization phase, it will receive attribute requests from RI. Those request include the handle as proof of identity, which will be used by the IdP to select the user attributes to be revealed.
- *BE in RI*. This component acts as the bridge between both institutions during the authorization phase. The remote RADIUS server, once the user is authenticated, will ask the local BE about the user attributes, defined in this home domain, in order to be able to take the right decision. Once the BE has obtained those attributes, it will ask the PDP entity in order to know the obligations or properties to be applied to the network connection, and will forward those properties to the RADIUS server. The BE has to be extended to support the communication with the RADIUS server and to manage the authentication handle. In order to allow an easy integration and the minimum impact over *eduroam*, the selected communication protocol between RADIUS and BEs is LDAP.
- *Policy Decision Point* (*PDP*). This new module is responsible for taking the authorization decisions about users based on a *Resource Access Policy*. Basically, this policy defines which users attributes are required to enforce specific properties or obligations in some resources. The PDP receives the requests from its local BE, making this process transparent to the RADIUS server.
- *Identity Provider* (*IdP*). This module is responsible for providing information about the users belonging to the institution, and it is institution dependent. During the authentication phase, this module is in charge of generating authentication statements, and further on, it will be able to disclose the user attributes by means of the authentication handle.

Once the main elements have been defined, the next section describes the interaction among them and the profile defined to manage the authorization process in *eduroam*.

6.1. Protocols and profiles

As previously described, this work proposes a two steps architecture to provide authentication and authorization in *eduroam*. This section describes in detail both steps including the communication protocols and the information exchanged between components.

Fig. 4 shows the network authentication phase proposed by DAMe. This phase starts when the user requests access to the *eduroam* network in a remote institution. In the usual case, the user presents his authentication credentials, which are composed by his email address and password. The remote RADIUS server, by means of the email domain identifier, recognizes he is a foreign user and, through the *eduroam* network, redirects the user to his home institution.

The home RADIUS server, after authenticating the user, will invoke, by means of a SAML *AuthenticationQuery* message, the IdP in order to get an authentication statement. This query includes the user's subject and the authentication method used by the server. This step is necessary in order to link the authentication statement with a further attribute query, and this information is centralized in the IdP. As previously described, the communication between the RADIUS server and IdP is done by means of the BE, using SOAP as communication protocol.

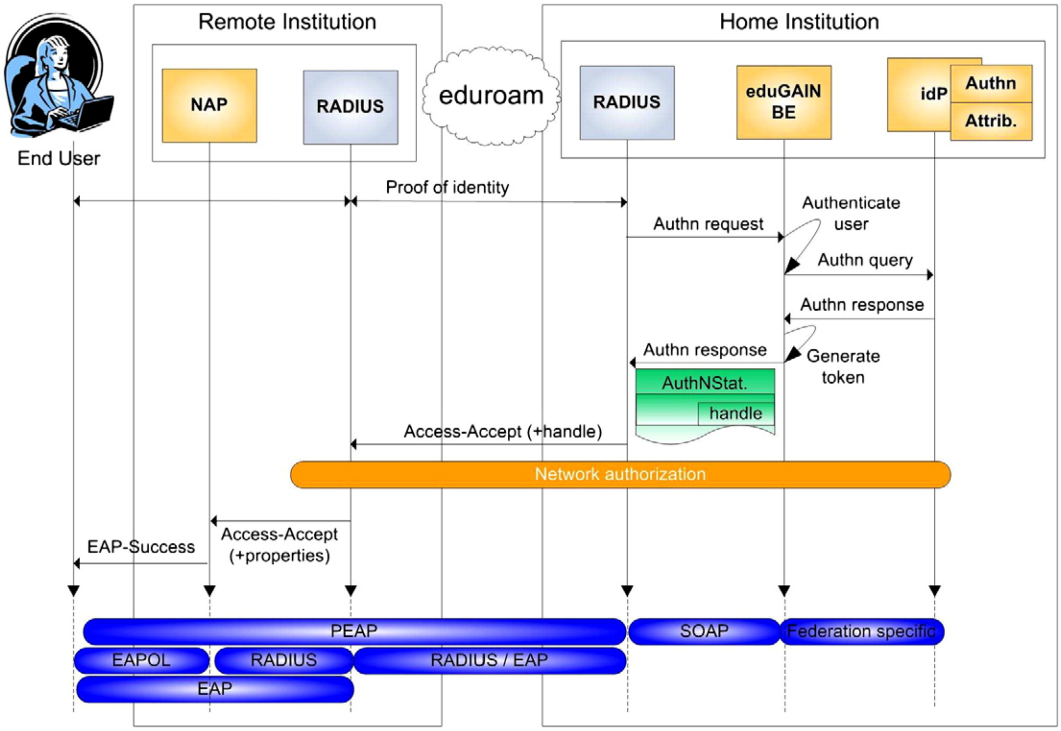


Fig. 4. Network authentication.

The IdP generates a SAML *AuthenticationStatement* sentence and sends it back to the BE. The communication between these modules will depend on the IdP implementation. For example, if Shibboleth or NAS-SAML are used then this communication is made through HTTP.

Once the home BE receives the authentication statement, it will generate an authentication handle, which will be used during the authorization phase. The remote BE forwards the response (including the new handle) to the RADIUS server, which will send a RADIUS *Access-Accept* message to the remote RADIUS server. The handle, usually the user's subject, can be forwarded to the remote institution in the *Access-Accept* message.

At this point, the remote RADIUS server knows that the user has been successfully authenticated and, before sending the EAP-success message to the user, it might launch the authorization phase, Fig. 5.

In this second step, the RADIUS server will ask for the network properties or obligations to be applied to the user's connection, which are defined upon the user attributes. The RADIUS server delegates the process of obtaining the user attributes and checking the properties to be applied to the local BE, which will act as follow.

The RADIUS server invokes this process by means of a LDAP connection to the BE. It will send an LDAP *SearchRequest* message including the authentication handle, the target resource (*network*) and the required action (*access*). Then, the remote BE sends a SAML *AttributeQuery* message (as described in eduGAIN) including all this information to the home BE. It is worth noting that the location of the home BE could be obtained either from the handle or from the MDS service, as proposed by eduGAIN.

The home BE, after receiving the query, will forward it to the corresponding attribute authority, in this case the IdP. As before, the communication protocol between BE and IdP will depend on the implemented technology.

The IdP, by means of the handle, selects the user attributes and, optionally, could use an attribute release policy to check which ones can be revealed to the remote institution. Finally, it generates a SAML *AttributeStatement* sentence including the selected attributes, which is sent back to the remote BE.

Once in the remote institution, the BE, using the NAS-SAML PDP entity, will send an authorization decision query in order to know the set of properties that have to be applied to the user network connection. This query includes the user subject and attributes, the target resource and the required action. The communication between the BE and PDP is made by means of SAML *AuthorizationDecisionQuery/Statement* messages, transported over SOAP, as described in the NAS-SAML proposal.

The authorization decision process is leaded by a *Resource Access Policy*, described in [9], which includes the set of network properties as XACML obligations. Once selected those properties, they are forwarded to the RADIUS server by means of a LDAP *SearchResult* message, which will be the responsible for enforcing them into the AP. Examples of those properties are the *Session-Timeout*, *MaxBandwidth*, etc.

7. Related work

Internet 2 has defined a similar proposal for carrying SAML statements over RADIUS [5]. This proposal defines a roaming scenario similar to *eduroam*, where RADIUS servers forward the authentication request to the user's home institution for authentication purposes. Once the user has been authenticated, a name identifier value for the user is sent back to the remote RADIUS server.

The main differences between DAMe's proposal and Internet2's is that the latter is closely related to one particular technology, Shibboleth, as new attributes are defined taking into account several Shibboleth details. Moreover, no authorization engine or policy is provided in order to obtain authorization decisions.

However, the proposal presented in this paper is closely related to eduGAIN, a generic authentication and authorization infrastructure able to support several federation technologies, not only Shibboleth. Additionally, a complete authorization back-end with XACML

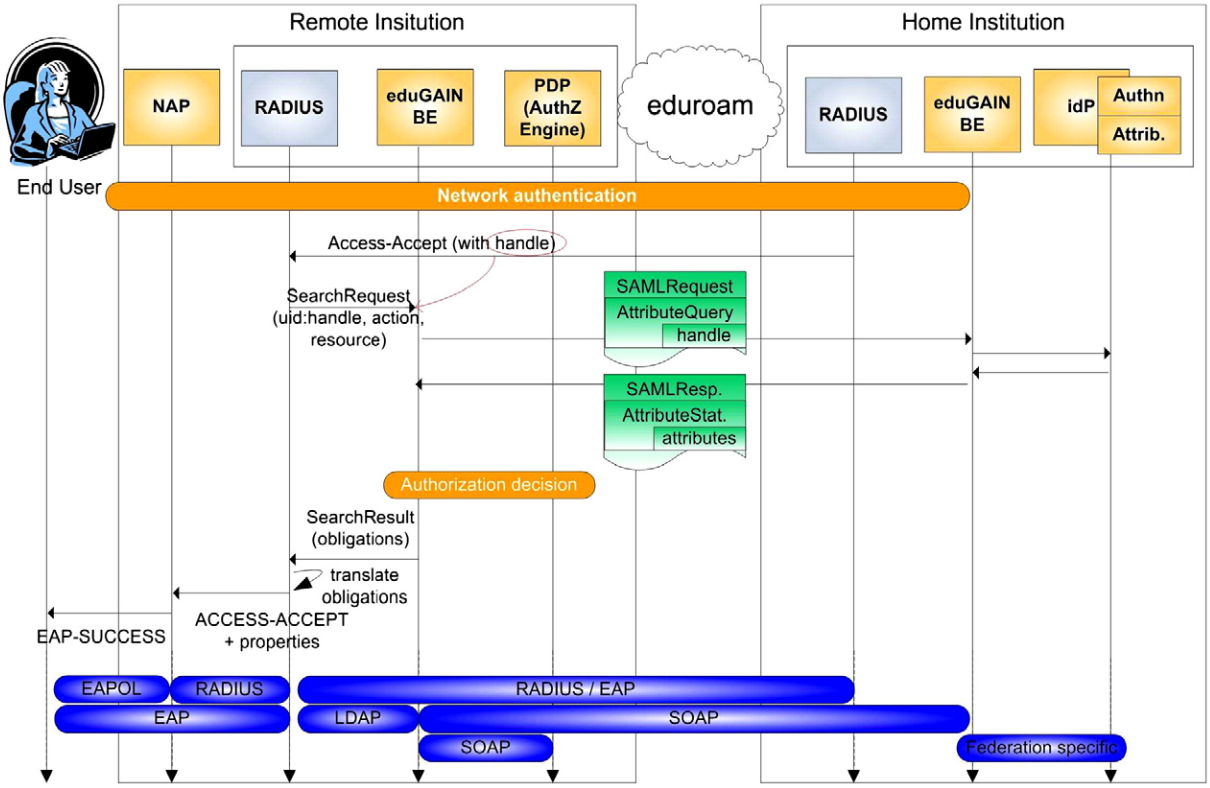


Fig. 5. Network authorization.

support and eduGAIN-aware is provided to help the RADIUS servers during the authorization phase.

8. Conclusions and future work

The authorization service defined in *eduroam* is based on both NAS-SAML and eduGAIN proposals. This proposal defines the architecture components and the whole access control process in two steps: authentication, through the underlying RADIUS infrastructure; and authorization, through eduGAIN. Although this two-steps approach implies a higher impact on the latency, it allows institutions to keep the traditional authentication process almost unaltered, which is one of the main objectives in this kind of widely spread scenarios.

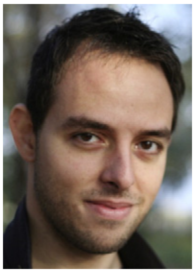
As a statement of direction, the main objective is to set up this new proposal in the real scenario defined by *eduroam*. It will imply a step-by-step process in order to allow participants institutions to add those new components to its infrastructures and to do not interfere in the normal use of *eduroam*.

DAMe objectives also cover aspects such as to provide a real Single Sign On, from a global point of view. That is, users will be authenticated once, during the network access control phase. Next, having authenticated to get onto the network, that authentication will automatically fetch the necessary eduGAIN-signed tokens so that there will be no need to repeat the login at the application layer. DAMe also plans to use the AAA network and the related authorization information to provide authorization mechanisms to application-level services, not only to the network access service.

References

[1] A. Anderson, et al., EXtensible Access Control Markup Language (XACML) Version 1.0, OASIS Standard, February 2003.
[2] al. J. Beatty, Liberty protocols and schema specification version 1.1, May 2005.
[3] L. Blunk, J. Vollbrecht, Extensible Authentication Protocol (EAP). Internet Engineering Task Force, Request for Comments (RFC) vol. 2284 (March 1998).
[4] S. Cantor, T. Scavo, Shibboleth architecture, Technical Overview, June 2005.
[5] S. Carmody, Radius Profile of SAML. Revision 2, October 2006 http://stc.cis.brown.edu/stc/Projects/Projects-using-Shib/eduRoam/Radius-SAML-Profile-v1.html.
[6] Dame Project, Julio 2007. http://dame.inf.um.es.
[7] DAMe conversions, From Shibboleth and PAPI authentication to eduGAIN SSO token, June 2007 http://dame.inf.um.es/.
[8] LAN MAN Standards Committee of the IEEE Computer Society, IEEE Draft P802.1X/D11: Standard for Port based Network Access Control, March 2001.
[9] G. López, O. Cánovas, A.F. Gómez, Use of XACML policies for a network access control service, Proceedings 4th International Workshop for Applied PKI, IWAP 05, IOS Press, 2005, pp. 111–122.
[10] G. López, O. Cánovas, A.F. Gómez, J.D. Jimenez, R. Marín, A network access control approach based on the AAA architecture and authorization attributes, Journal of Network and Computer Applications JNCA, vol. 30, Elsevier, 2007, pp. 900–919.
[11] G. López, O. Cánovas, A.F. Gómez-Skarmeta, S. Otenko, D. Chadwick, A heterogeneos network access service based on PERMIS and SAML, In Proceedings 2nd European PKI Workshop, Lecture Notes in Computer Science, vol. 3545, Springer, 2005, pp. 55–72.
[12] D. Lopez, PAPI: simple and ubiquitous access to Internet information servers, Proceedings of 4TH International JISC/CNI Conference, June 2002.
[13] E. Maler, P. Mishra, R. Philpott, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)v1.1, OASIS Standard, September 2003.
[15] D.R. Lopez, A. Solberg, M. Stanica, eduGAIN Profiles and Implementation Guidelines, December 2006 GN2 JRA5. Geant 2.
[16] A. Rubens, C. Rigney, S. Willens, W. Simpson, Remote Authentication Dial In User Service (RADIUS), June 2000 RFC 2865.
[17] M. Sánchez, G. López, O. Cánovas, A.F. Gómez-Skarmeta, Grid authorization based on existing AAA architectures, Proceedings of 4The Fourth International Workshop on Security In Information Systems WOSIS-2006, May 2006.
[18] Trans-European Research and Education Networking Association (TERENA) home page. http://www.terena.nl.
[19] K. Wierenga, L. Florio, Eduroam: past, present and future, TERENA Networking Conference, 2005.

Gabriel López is an assistant professor in the Department of Information and Communications Engineering of the University of Murcia. His research interests include network security, PKI, and IPv6. He received his MS and PhD in computer science from the University of Murcia.



Óscar Canovas is an assistant professor in the Department of Computer Engineering at the University of Murcia. His research interests include public PKI, authorization management systems, and network access services. He received his MS and PhD in computer science from the University of Murcia.

Antonio F. Gómez-Skarmeta is an associate professor at the University of Murcia, Spain. He received an MS in computer science from the University of Granada and a PhD in computer science from the University of Murcia. His research interests include distributed artificial intelligence and computer networks security.

Manuel Sánchez is a researcher in the Department of Information and Communications Engineering of the University of Murcia. His research interests include network security and Grid Computing. He received his MS in computer science from the University of Murcia.