A Proposal for Extending the Eduroam Infrastructure with Authorization Mechanisms

Manuel Sánchez[1], Gabriel López[1], Óscar Cánovas[2] and Antonio F. Gómez-Skarmeta[1]

[1] Department of Information and Communications Engineering
[2] Department of Computer Engineering
University of Murcia, Spain

Abstract. Identity federations are emerging in the last 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 a more grained access control and value added services. Therefore, additional information, such as user attributes, need to 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. This authorization framework has been integrated by means of the NAS-SAML infrastructure, which defines a network access control service based on SAML and the AAA architecture.

1 Introduction

In the last years, we have experienced the emergence of federated approaches to resource sharing. In these federations, trust links are established among different autonomous organisations in order to grant users in any of them access to shared resources with a single identity, stated by the organisation the user belongs to. Important examples of these approaches are the establishment of academic federations worldwide and the concepts around Grid Computing.

In fact, many aspects of this federated approach have been addressed by several projects, as for instance Shibboleth [1] or Liberty Alliance [2]. However, other aspects generally related with integral identity management are still open, especially those related to user authorization. Indeed, authorization is a critical feature in this environment because when an organization offers its resources to the users belonging to other domains, it wants to be sure that only allowed users are able to perform the set of allowed actions over each resource.

This service level agreement among different organizations requires several efforts related to user mobility, exchange of security information, integration of heterogeneous proposals, etc. Concerning to user mobility, the TERENA Mobility Task Force [3] provided a forum for exchanging experiences and knowledge about the different roaming development activities in the European Union. As a result of this effort, this task force

Sánchez M., López G., Cánovas Ó. and F. Gómez-Skarmeta A. (2007).
A Proposal for Extending the Eduroam Infrastructure with Authorization Mechanisms.
In *Proceedings of the 5th International Workshop on Security in Information Systems*, pages 23-32
DOI: 10.5220/0002408400230032

defined and tested an inter-NREN roaming architecture, called eduroam [4], based on AAA servers (RADIUS [5]) and the 802.1X [6] standard. Eduroam allows users of participating institutions to access the Internet at other participants using their home institution's credentials, all this with a minimal administrative overhead.

Depending on local policies at the visited institutions, eduroam participants may also have additional resources at their disposal. Therefore, it would be desirable to extend the eduroam architecture with authentication and authorization mechanisms in order to exchange additional information (credentials) about the users that might be used at service-level. The main objective of the DAMe project (Deploying Authorization Mechanisms for federated services in the eduroam architecture) [7] is to define this unified authentication and authorization system for federated services hosted in the eduroam network, in order to allow the use of those user authorization credentials previously described. Those federated services can range from network access control to distributed services like Grid Computing.

Since eduroam already defines how the authentication process is managed inside a federation, the main challenge of DAMe is to define how the authorization process will be included in this infrastructure. In order to accomplish this, DAMe will make use of the NAS-SAML infrastructure [8]. NAS-SAML is a network access control system based on the AAA architecture and authorization attributes. The proposal is based on the SAML (Security Assertion Markup Language) [9] and the XACML (eXtensible Access Control Markup Language) [10] standards, which are used for expressing access control policies based on attributes, authorization statements, and authorization protocols.

The rest of this paper is structured as follow. Section 2 provides an overview of the eduroam service, which defines the underlying roaming infrastructure. Section 3 describes the NAS-SAML network access control service, which will provide authorization services to the eduroam network. Section 4 points out the set of requirements derived from the integration of both systems and section 5 describes the proposed architecture. Finally, we conclude the paper with our remarks and some future directions.

2 The Eduroam Service

Eduroam (Education Roaming) is an inter-institutional roaming service based on the 802.1X architecture and a hierarchical RADIUS-based infrastructure. This initiative allows mobile users of participating institutions to access the Internet at different locations using their home institution's credentials, all this 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 (NREN's) belonging to the eduroam infrastructure are connected to this one. Finally, each institution willing to join eduroam connects its own RADIUS server to the national server of its NREN.

Figure 1 depicts a user from Institution A who wants to get access to the wireless network in Institution B, both pertaining to the eduroam federation. In this situation, access control is carried out following the 802.1X standard. That is, the user associates with the wireless access point (AP), which contacts its local RADIUS server in order to authenticate the user. Once this server identifies that the user belongs to a different

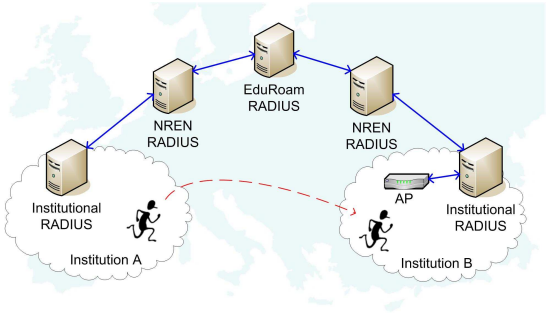

Fig. 1. Eduroam infrastructure.

domain, based on the user identifier for example, the authentication request is forwarded through the RADIUS hierarchy to the server in the user's home institution. Then, the user is authenticated and the response is routed back to Institution B, where the AP enables the requested connection.

The 802.1X standard defines the use of EAP (Extensible Authentication Protocol) for authentication purposes since it allows different authentication mechanisms. Therefore, institutions can use any of the different authentication methods depending on the required security level. For example, users can make use of login and password (EAP-MD5), or digital certificates may be required both for users and servers (EAP-TLS).

Nowadays, more than 350 institutions over 19 countries (European and Australian-Pacific) participate in the eduroam initiative. Moreover, the Internet2 Working Group has started a similar RADIUS infrastructure to incorporate US into eduroam.

However, the deployed eduroam infrastructure is only useful for user authentication. Target institutions cannot provide different services depending on the particular user requesting the service. They enable the same kind of connection since no additional information (e.g. user's attributes) is taken into account. It would be desirable that target institutions offer differentiated services based on some information about the user defined in his home institution. Consequently, additional data about users should be exchanged between institutions in some way, which will be used next in the target institution to provide the suitable services to the user.

3 SAML-Based Network Access Control Architecture

Traditionally, network access systems have been based only on user's identity, what is useful for organizations which are concerned about the real identity of the requester. There are other organizations where users are classified according to their administrative tasks or some others internal criteria. In those scenarios, the user's identity could not be enough to grant the access to the resource being controlled, since we should know the attributes defining the user's profile in order to offer the right service. Therefore, a system able to exchange the set of attributes specifying those privileges [11] is needed.

NAS-SAML [8] is a network access control approach based on X.509 identity certificates and authorization attributes. It is based on the SAML and the XACML standards, which will be used for expressing access control policies based on attributes, authorization statements, and authorization protocols. Authorization is mainly based on the definition of access control policies [12] including the sets of users pertaining to different subject domains which will be able to be assigned to different roles in order to gain access to the network of a service provider, under specific circumstances.

The system operates as follows. Every end user belongs to a home domain, where he was given a set of attributes stating some additional properties or roles he plays. When the user requests a network connection in a particular domain by means of an 802.1X connection, the request is captured by an AAA (Authentication, Authorization and Accounting) [13] server located in the target domain. That server makes a query to obtain the attributes linked to the user from an authority responsible for managing them, located in the user's home domain. Alternatively, following a push approach, the user can present his attributes. The communication between different domains is carried out using the DIAMETER protocol [14]. Finally, the AAA server sends an authorization decision query to a local PDP (Policy Decision Point) entity, and that element provides an answer indicating whether the attributes satisfy the resource access control policy. Furthermore, that policy can also establish the set of obligations derived from that decision, for example some QoS parameters, security options, etc. This general scheme works both in single and inter-domain scenarios.

NAS-SAML has been also integrated with other authorization systems, such as PERMIS [15], by means of a credential conversion service [16] used to translate authorization credentials from one source domain to a target one. Some additional integrations prototypes have been defined also for Grid Computing [17] environments.

4 Analysis of the Requirements Derived from Integrating eduroam and NAS-SAML

The integration of NAS-SAML into eduroam as authorization service can be carried out in several ways, depending on the requirements imposed by the participating institutions or the AAA implementation. On the one hand, the target institution should receive the additional information describing the user from his home institution. On the other hand, that information should be used in the target institution to determine whether the user can access to the service being requested.

A first approach (called *merged authorization*) allows the home institution to return the information about the user in the same channel established for authentication. That is, when the home RADIUS server receives the authentication request from the target institution, it forwards the request to the NAS-SAML infrastructure, which authenticates the user and retrieves some additional attributes. That information can be encoded in the response as RADIUS attributes. Since NAS-SAML works with DIAMETER, the RADIUS-DIAMETER translator described in [18] should be used as a gateway to access the NAS-SAML architecture. Once the target RADIUS server obtains that information, a query to a local element of the NAS-SAML infrastructure, the PDP, is performed in order to obtain the authorization decision. Finally, if the decision

is permit, the response and the appropriate RADIUS attributes are returned to the AP. This approach can be considered optimal regarding inter-domain communications. The main drawback of this alternative is the extension and, therefore, the use of non standard RADIUS attributes to transport the information about users between the different institutions, which should be by-passed at any intermediary RADIUS server.

In order to avoid the modification of the authentication process defined in eduroam by introducing non standard attributes, a second alternative can be defined (called *independent authorization*). The authorization process should start once the authentication has been established following the current eduroam profiles. That is, once the target RADIUS server receives the authentication response, the authorization stage is initiated to determine the type of service to be provided. This stage is also performed through NAS-SAML. First, to retrieve the information about the user from the home institution, and then to obtain the authorization decision in the target institution, as we commented above. Whereas this approach does not modify the authentication process, it introduces the need for the definition of an interface between the RADIUS server and the NAS-SAML architecture (DIAMETER-based) for requesting authorization decisions and obligations derived from that decision. Moreover this approach needs two inter-domain communications, the former for authentication and the later for authorization, therefore introducing an additional overhead.

A third alternative, following the same approach of differentiated authentication and authorization steps, might be obtained extending the RADIUS protocol with a new profile defining new attributes and messages. In this way, the authorization stage would make use of the RADIUS protocol as a transport mechanism to obtain the information needed for the authorization process. This proposal is being developed by Internet 2 [19].

5 Proposed Architecture

Before providing the definition of the solution, it is necessary to take into account that eduroam has been already deployed. In other words, hundreds of institutions are using it and, therefore it is necessary to introduce changes gradually, maintaining backward compatibility. In this way both alternatives has been designed, but only the independent authorization has been implemented at the moment since it is the most suitable for initial testing in DAMe.

To extend the current eduroam infrastructure in order to offer authorization mechanisms with the minimum impact in the institutions willing to continue using the standard process, it has been decided to preserve the current eduroam authentication mechanism in the implemented approach (*independent authorization*) and to deploy a new authorization infrastructure. In this way, using this alternative institutions can decide whether they want to use an extended RADIUS server connected to the NAS-SAML architecture (authentication and authorization), or a standard one (only authentication). Figure 2 shows this approach.

As we can see, when an institution wants to join eduroam and support user's authorization, it has to deploy a DIAMETER server, a Policy Decision Point (PDP), and an Attribute Authority (AA).

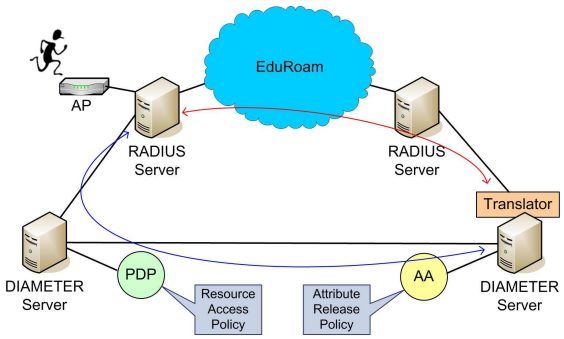

Fig. 2. Implemented architecture (independent authorization).

According to this approach, Figure 3, once the roaming user is authenticated following the standard eduroam mechanism, the target RADIUS server uses the NAS-SAML infrastructure to lead the authorization process. Therefore, the DIAMETER home server is consulted about the user's attributes and, once this information is recovered, an authorization decision is obtained using the PDP. Moreover, a set of obligations can be returned along with the authorization decision containing some specific network properties to be enforced by the access point.

More specifically, as detailed in [8], the target DIAMETER server sends a message to the home server including a *SAMLAttributeQuery* sentence, which contains the user's identity. Then, this query is forwarded to the Attribute Authority (AA), which consults an *Attribute Release Policy*. This policy, based on XACML, specifies the user's attributes that can be released to that target institution. Next, those allowed attributes, and their corresponding values, are sent back by means of a *SAMLAttributeStatement* sentence. Once the attributes are recovered at the target institution, a *SAMLAuthorizationDecisionQuery* request is sent to the Policy Decision Point (PDP). This query contains the user's identity, the resource identifier, the action being requested, and the user's attributes. Using this information, the PDP is able to obtain the authorization decision according to the *Resource Access Policy*, also based on XACML technology. Finally, the PDP returns a *SAMLAuthorizationDecisionStatement* response, which might contain specific obligations. The mechanism used by the target DIAMETER server to find out the home server can be based on the user identifier, as defined in [14].

Finally, the last alternative, called *merged authorization*, implies several changes in the RADIUS hierarchy, due to it is necessary to configure intermediate proxy servers to do not discard the RADIUS attributes carrying the user's data. Moreover, institutions need to introduce a new element in its infrastructure, the RADIUS-DIAMETER translator. In this way, once the home RADIUS server receives the authentication request from the target institution, this request is forwarded to the NAS-SAML infrastructure through the translator, as described in section 4. As we can see in Figure 4, the DIAMETER server authenticates the user and queries the Attribute Authority, using a *SAMLAttributeQuery* request, in order to obtain the set of attributes which can be disclosed to the specific target institution according to the *Attribute Release Policy*. The resulting SAML attributes are transported into the DIAMETER-SAML messages [8],

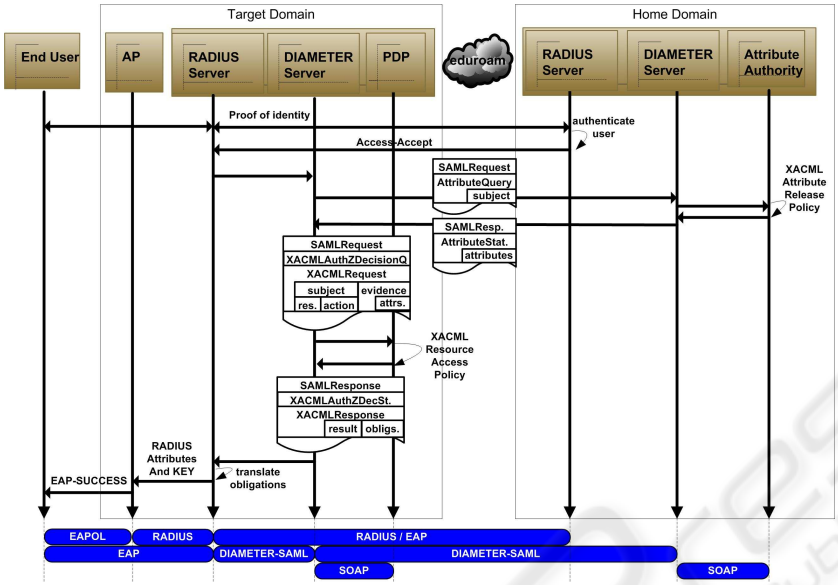

Fig. 3. Collaboration diagram (independent authorization).

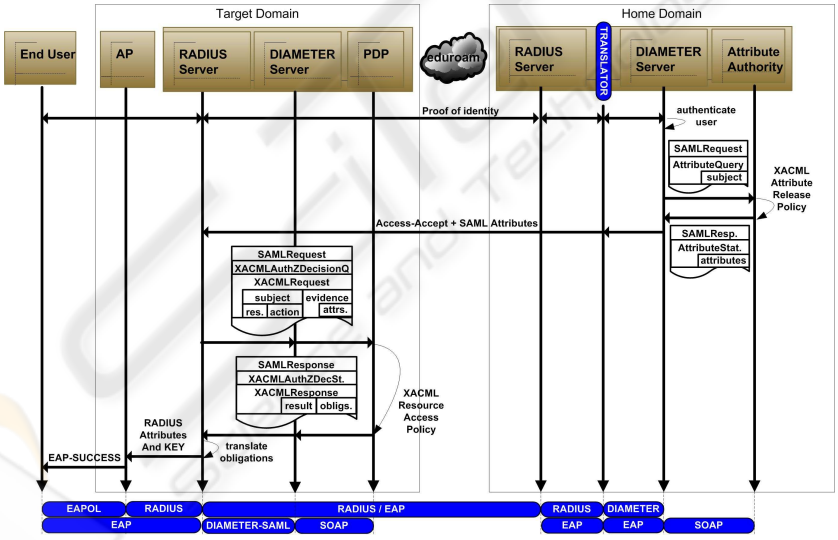

Fig. 4. Collaboration diagram (merged authorization).

and then translated into RADIUS attributes by the translator. Finally, when the target RADIUS server receives this message, contacts with its local NAS-SAML gateway to obtain an authorization decision as already explained.

Regarding the merged authorization deployment, once the first approach is working it is possible to introduce the RADIUS-DIAMETER translator in home institutions. Therefore roaming users can be authenticated by the DIAMETER servers and its attributes be returned directly. Then, if the new RADIUS attributes are not discarded at intermediary proxy elements because they understand these attributes, it is not needed a new inter-domain communication in order to perform the authorization process. Only if they were discarded, that information will be requested by the target RADIUS server through NAS-SAML, using therefore the independent authorization.

6 Related Work

Nowadays, when talking about access control and authorization, one of the main alternatives is Shibboleth [1]. This proposal defines an access control system for web services by means of a SAML-based authorization infrastructure. Its main goal is to exchange information about users to determine whether they are allowed to access to a target resource. The user information, which can be represented as attributes, is defined in the user home domain. In this way, Shibboleth enables the creation of identity federations, in such a way that different domains exchange information about the user's identity in a reliable way. Besides, due to the authorization decision is based on the user's attributes, it is not necessary to disclose the user's identity. Therefore it is necessary to take into account that Shibboleth is a technology that provides both authentication and authorization management for federations. Besides, these two processes are closely related by means of a specific kind of user's identifiers generated in the authentication phase which is used later in the authorization phase to locate the user's attributes. Eduroam only needs to be extended with an authorization infrastructure without modify the authentication process. Therefore is not possible to include the authorization mechanism of Shibboleth without altering the authentication process in eduroam. Furthermore, Shibboleth is oriented to web environments, so its authentication and authorization processes are based on the use of secure web pages, cookies and redirections. Those technologies are not appropriate to be used in eduroam since it is mainly a network access control infrastructure based on the 802.1X standard. However, it could be possible to make them interoperable by means of proposals such as eduGain [20] or the RADIUS-SAML profile detailed below.

Internet 2 has defined a similar proposal for carrying SAML statements over the RADIUS protocol [19] is being developed. This proposal defines a roaming scenario similar to eduroam, where RADIUS servers forward the authentication request to the user's home domain for authentication purposes. This scenario also specifies the possibility of including an attribute request during the authentication stage. In this case, once the user is successfully authenticated, the home RADIUS server returns, besides the authentication response, a new generated user identifier and the URL of the local Attribute Authority. Then, the target RADIUS service can ask the specified Attribute Authority for the user's attributes using a SAML query. This proposal seems similar to our merged authorization alternative, but they are slightly different since the information included inside the authentication response is just a link to an Attribute Authority. That is, a new query is necessary to recover the user's attributes. In this sense, this proposal is quite

similar to the independent authorization alternative since authentication and authorization are performed at different stages. Consequently, it does not provide the benefit of needing only one inter-domain communication to authenticate and authorize the user and, additionally, it requires some modifications in the RADIUS protocol.

7 Conclusions and Future Work

Current federation initiatives are mainly based on solutions deploying access control to protected resources only by means of identity credentials, without taking into account additional information about the user, such as the affiliation or role in his home domain, or additional properties that can be useful in order to offer differentiated services.

This paper presents how eduroam, a real and widely deployed user federation for an inter-NREN network roaming service, can take advantage of the use of authorization services in order to offer a more grained network access control process.

This authorization service is based on NAS-SAML, and this paper defines the architecture components that must be used in order to integrate both scenarios. The proposed architecture provides two different alternatives in order to take into account the requirements of the involved institutions, such as the level of intrusion in the already deployed authentication infrastructure or latency requirements. The first approach (merged authorization) allows a remote domain to obtain authorizations credentials in the same authentication channel, so it implies minimum latency requirements. On the other hand, it should make use of non standard RADIUS attributes in order to transport authorization credentials, which could be removed in intermediate servers. The second approach (independent authorization) defines the whole access control process in two steps: the first one is the authentication process, through the underlying RADIUS infrastructure; the second one is the authorization process, through the NAS-SAML infrastructure. This two-steps approach implies a higher impact on the latency but allows institutions to keep the traditional authentication process unaltered.

As a statement of direction, beyond the integration of NAS-SAML into the eduroam infrastructure, DAMe objectives also cover aspects such as the integration of the authorization process based on NAS-SAML with the eduGain [20] proposal, in order to define a generic framework to allow heterogeneous federations to share a common authorization infrastructure. Finally, it 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.

Acknowledgements

This work has been partially funded by Daidalos FP6-IP-506997 and DAMe.

References

1. T. Scavo, S.C.: Shibboleth Architecture. Technical Overview. (2005) Working Draft 02.
2. J. Beatty, a.: Liberty Protocols and Schema Specification Version 1.1. (2003) Liberty Alliance Project.
3. : Trans-European Research and Education Networking Association (TERENA) home page. (`http://www.terena.nl`)
4. Wierenga, K., Florio, L.: Eduroam: past, present and future. In: TERENA Networking Conference. (2005)
5. C. Rigney, S. Willens, A.R., W.Simpson: Remote Authentication Dial In User Service (RADIUS). (2000) RFC 2865.
6. LAN MAN Standards Committee of the IEEE Computer Society: IEEE Draft P802.1X/D11: Standard for Port based Network Access Control. (2001)
7. : Dame Project. (2006) `http://dame.inf.um.es`.
8. López, G., Cánovas, O., Gómez, A.F., Jimenez, J.D., Marín, R.: A network access control approach based on the aaa architecture and authorzation attributes. Journal of Network and Computer Applications JNCA (2006) To be published.
9. Eve, M., Prateek, M., Rob, P.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)v1.1. (2003) OASIS Standard.
10. et al., A.A.: EXtensible Access Control Markup Language (XACML) Version 1.0. (2003) OASIS Standard.
11. Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D., Chandramouli, R.: Proposed nist standard for role-based access control. ACM Transaction on Information and System Security **4** (2001)
12. López, G., Cánovas, O., Gómez, A.F.: Use of xacml policies for a network access control service. In: Proceedings 4th International Workshop for Applied PKI, IWAP 05, IOS Press (2005) 111–122
13. de Laat, C., Gross, G., Gommans, L., Vollbrecht, J., Spence, D.: Generic AAA Architecture. (2000) RFC 2903.
14. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J.: DIAMETER base protocol. (2003) RFC 3588.
15. López, G., Óscar Cánovas, Gómez-Skarmeta, A.F., Otenko, S., Chadwick, D.: A heterogeneos network access service based on permis and saml. In: Proceedings 2nd European PKI Workshop. Volume 3545 of Lecture Notes in Computer Science., Springer (2005) 55–72
16. Cánovas, O., Lopez, G., Gómez-Skarmeta, A.: A credential conversion service for saml-based scenarios. In: Proceedings First European PKI Workshop. Volume 3093 of Lecture Notes in Computer Science., Springer (2004) 297–305
17. Sanchez, M., Lopez, G., Cánovas, O., Gómez-Skarmeta, A.: Grid Authorization Based on Existing AAA Architectures. (2006) Submitted to The Fourth International Workshop on Security In Information Systems WOSIS-2006.
18. Calhoun, P., G.Zorn, Spence, D., Mitton, D.: Diameter Network Access Server Application. (2005) RFC 4005.
19. Carmody, S.: Radius profile of SAML. Revision 2. (2006) `http://stc.cis.brown.edu/~stc/Projects/Projects-using-Shib/eduRoam/Radius-SAML-Profile-v1.html`.
20. López, D.R., Macias, J., Molina, M., Rauschenbach, J., Solberg, A., Stanica, M.: Deliverable DJ5.2.3.1: Best Practice Guide - AAI Cookbook - First Edition. (2006) GN2 JRA5. Geant 2.