

08.01.07

Deliverable DJ5.3.1: Documentation on GÉANT2 unified Single Sign-On (uSSO) Requirements



Deliverable DJ5.3.1

Contractual Date: 31/01/07
Actual Date: 01/02/07
Contract Number: 511082
Instrument type: Integrated Infrastructure Initiative (I3)
Activity: JRA5
Work Item: 3 (SSO)
Nature of Deliverable: R (Report)
Dissemination Level: PU (Public)
Lead Partner: SURFnet
Document Code: GN2-06-261v4

Authors: B. Kerver (SURFnet), M. Stanica(DFN), J. Rauschenbach(DFN), K. Wierenga (SURFnet)

Abstract

The objective of this deliverable is to identify and to classify the requirements of a *unified Single Sign-On* (uSSO) solution that GN2 JRA5 is going to build in order to provide a method to sign-on for location-independent access to both applications and (network-) services, as provided by the GN2 Roaming Service *eduroam* and AAI Infrastructure *eduGAIN*.

Project:	GÉANT2
Deliverable Number:	DJ5.3.1
Date of Issue:	01/02/07
EC Contract No.:	511082
Document Code:	GN2-06-261v4

Table of Contents

0	Executive Summary	1
1	Introduction	2
2	Scenario for uSSO	4
	2.1 The general uSSO Problem	4
	2.2 The uSSO scenario for access to network and resources	6
3	SSO Requirements	10
	3.1 Security Requirements	10
	3.2 Standards Compliance and Integration	11
	3.3 Operational Requirements	12
	3.4 Organisational Requirements	12
	3.5 Authentication and Authorisation Mechanisms	13
4	Conclusions	14
5	References	15
6	Acronyms	16

Table of Figures

Figure 2.1: Overview of components in eduroam and eduGAIN	5
Figure 2.2: Communication pattern for network and web resource access at two different RIs	7

0 Executive Summary

This document aims at setting a base for the development of a unified Single Sign-On solution within JRA5, which is meant to combine access to network and (web) resources. The results of this work are oriented towards the European research and education community, intending to facilitate interoperability between existing national federations.

An important characteristic arising from this context is the existence of heterogeneous environments, whereas previous SSO implementations are strongly dependent on homogenous IT infrastructures. Consequently, uSSO will need to support multiple domains and AA systems for access to network and application resources. The uSSO solution builds on the eduroam and eduGAIN infrastructures developed in JRA5. Therefore, apart from the combination of requirements from roaming and AAI, further challenges and requirements are added in the process of integrating already existing architectures. Although the same generic functional components appear in both of these architectures, the resulting model has increased complexity arising from the need to integrate the different roaming and AAI technologies. A common electronic identity model needs to be shared between all institutions connected by the uSSO solution, and the ability to pass assertions for this identity from the network layer to the application layer needs to be supported.

The SSO architecture development will be covered in the next SSO deliverable, but some general assumptions and requirements on authentication and authorisation mechanisms are included here as a first outlook.

1 Introduction

Single Sign-On (SSO) means that upon one successful authentication a user is able to access all network and web resources for which they are authorised, without the need for any additional login. The data necessary for authentication is provided to the resource owner(s) by the SSO mechanism, this process being transparent to the user after their initial login.

The main advantages of SSO are efficiency (only one authentication needed) and ease for the user (only one password to remember). A possible disadvantage is that identity spoofing can lead to unjustified access to all resources for which a user is authorised.

Existing SSO solutions depend mostly on the presence of a homogenous IT infrastructure regarding the identity management (IdM) systems used and are generally based on one of the following approaches:

- *Web portals*: Upon primary authentication on a portal, the user is provided with a cookie that is used for authentication and access to all resources connected to the portal.
- *Ticketing system*: Within a network of resources connected by trust links and sharing a common user identity model, a user can authenticate with one of the resources and obtain a virtual ticket asserting their identity for all the other resources.
- *SSO client*: A program installed on the user's machine is in charge of providing the corresponding credentials to each resource being accessed; these credentials can be stored either locally or on single sign-on appliances or servers in the network.

In the JRA5 context, the absence of a homogenous IdM infrastructure poses significant challenges and is the reason why the above-mentioned approaches are not directly applicable. A new approach based on the federation concept involves the use of standard-based protocols to enable one application to assert the identity of a user to another application, thereby avoiding the need for repeated authentication. JRA5 intends to provide a SSO solution for the research and education community in Europe forming a heterogeneous environment with respect to identity management, hence the name of 'unified SSO' (uSSO).

Since the development of the uSSO solution is based on the eduroam and eduGAIN infrastructures, it is dependent on results from these first two work items and therefore started later. While eduroam is currently in the transition to service phase, eduGAIN implementation is progressing and approaching the test phase. The

practical experience accumulated in the roaming and AAI work items makes it possible to formulate the SSO requirements and investigate potential scenarios and architectural solutions.

This documents starts by describing a scenario for unified SSO and elaborates on the similarity of concepts in the underlying roaming and AA architectures. The resulting common and technology-specific requirements are then presented, as well as those arising from the need to integrate the already existing infrastructures eduroam and eduGAIN.

2 Scenario for uSSO

The purpose of this chapter is to illustrate the requirements on the uSSO, thus providing a scenario for the access to both network and application resources. The general (eduGAIN) AAI model is used as the framework.

2.1 The general uSSO Problem

The general problems that have to be solved for uSSO are the support of multiple domains and different authentication and authorisation systems for access to resources (including network), and the ability to pass on assertions from the network layer to the application layer. Whereas eduroam only focuses on access to network resources and eduGAIN focuses on access to (web) resources, the uSSO solution should be able to accommodate requirements from both fields and be in concordance with the infrastructures and solutions that have already been created within eduroam and eduGAIN. The uSSO solution should be transparent for the user and operating system independent.

Since the roaming and AAI requirements should both be fulfilled, the design model provided in [DJ5.2.1] “Documentation on GÉANT2 AAI Requirements” and [DJ5.1.2] “Documentation on GÉANT2 Roaming Requirements” is used again.

The scenarios below integrate some of the basic functional elements needed as a starting position for the discussion of the architectural design (next deliverable in the JRA5 uSSO work item).

The uSSO scenarios are based on the following assumptions:

- Any user U is given an appropriate digital identity by his home institution HI.
- Digital identities issued by the HI are trusted and valid in a federation of participating institutions.
- In particular, if U wants to access or operate on resource R, their digital identity has to be trusted by the resource owner or service provider in the resource institution RI.
- The control of the authorisation to access or operate on a resource R is decided (or delegated) by an Authorisation Service of the resource owner or service provider at the institution RI.

- A mechanism exists that enables the exchange of authentication and authorisation information between the Authentication and Authorisation Services of HI and RI. This mechanism is provided by a (con)federation interconnecting the participant federations and/or institutions.
- There is a confederation-aware AAI component, called “Local Federation Adaptor” (LFA), which decides whether an authentication request can be handled locally or whether support from the confederation is needed.

In order to allow controlled inter-domain usage of resources, a harmonised digital identity definition is necessary between the AAIs of the federation partners. The RI AAI, for each potential guest, has to trust the identity management procedures and the Authentication Service in the corresponding HI AAI. Therefore, an identity federation has to exist with the RIs and the HIs as members. Furthermore, it is necessary that the Authorisation Service in the RI AAI is able to discover and communicate with the Authentication Service in the HI AAI. To facilitate these two functions, the concepts of ‘federation’ and ‘confederation’ are used. The federation contains a trust fabric that interconnects the member AAIs and thus provides the RI with a link to the user’s HI. When the HI and RI are part of different federations, the trust fabric linking these federations and implicitly their participant institutions is provided by a confederation. The resulting model can be easily applied to the roaming case seeing the network as resource R. All the assumptions made are valid for network access and access to (web-) resources.

This model has been applied for the requirements of both eduroam and eduGAIN (see Figure 2.1). These infrastructures allow for the establishment of the trust links needed for connecting different AAIs. Both of them consist of the same basic set of functional elements: an identity provider (IdP) and a Local Federation Adaptor (LFA) as part of the AAI of the home institution (HI); generic federation services; a service provider (SP) and an LFA belonging to the AAI of the resource institution (RI); a user U with their specific client.

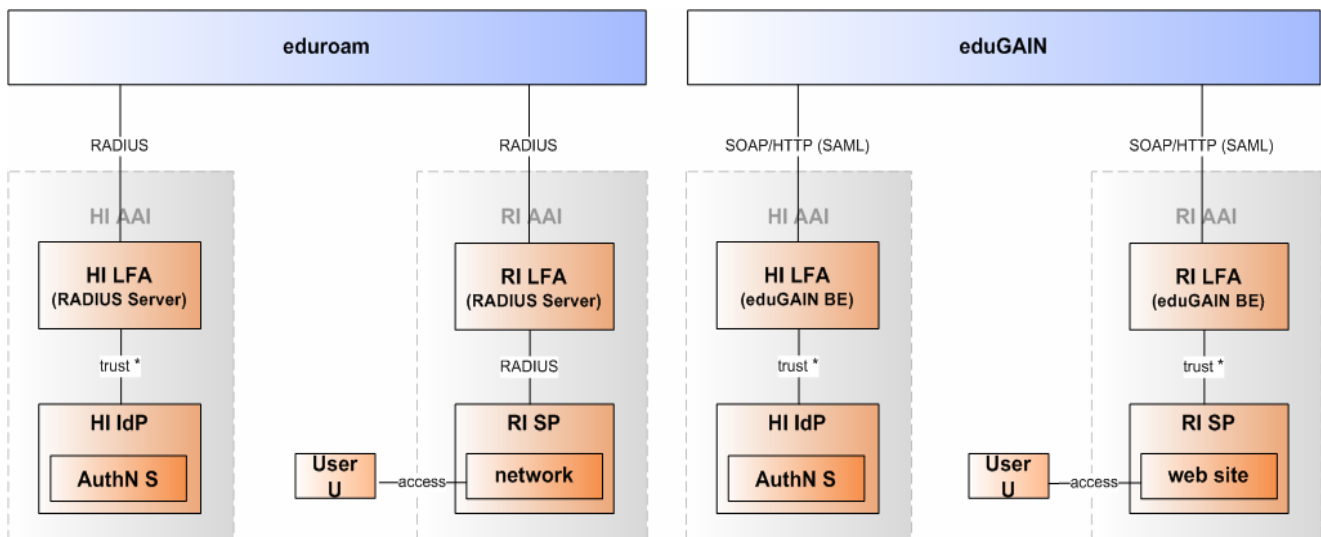


Figure 2.1: Overview of components in eduroam and eduGAIN

The eduroam infrastructure is based on the RADIUS protocol for transport of credentials, whereas EAP is used as the container for the credentials that are sent from the client to the IdP. The eduGAIN infrastructure is

Project:	GN2
Deliverable Number:	DJ5.3.1
Date of Issue:	01/02/07
EC Contract No.:	511082
Document Code:	GN2-06-261v4

designed as a generic AAI for access to (all kinds of) resources, in this example a web site. SAML is used as a container for the credentials that are provided by the client and are sent using either SOAP or HTTP as means of transport.

The trust relations within a federation's AAI (designated with 'trust*' in the figure above) are built by means of local mechanisms and protocols chosen by each institution and agreed upon by the federation. In the case of eduRoam, the connection between the IdP and the RADIUS Server can be established using LDAP or SQL. For eduGAIN, existing AAI implementations connecting the local IdPs and SPs to the Bridging Elements include Shibboleth, PAPI, A-Select, Feide/Liberty Alliance, etc.

2.2 The uSSO scenario for access to network and resources

The following scenario assumes support for existing NREN-specific roaming and AA solutions. However, these AA solutions might not be eduGAIN-enabled. For that reason, a Local Federation Adaptor is needed in order to connect them to a confederation established between non-eduGAIN-aware AA solutions. The LFA acts like a proxy-connector, performing all the required functions to enable inter-domain communication between existing AA systems. It is realized as a separate functional component for conceptual reasons; in later implementations a combination of this functionality with closely related components, such as the Authentication Service, will probably be chosen if efficiency and performance advantages can be proven.

There can be several alternative scenarios for uSSO: a simple scenario with just one Resource Institution that offers both network access and access to (web) resources, and a more complex scenario with two Resource Institutions in different federations. Besides this, the scenarios can be enhanced with authorization and/or local SSO provided by the visited Resource Institution. For better understanding of the concept a simplified common scenario is described, involving two RIs in different federations, but no authorisation. The challenge for uSSO lies not so much in supporting federated authentication and authorisation (this is typically handled by eduGAIN), but more in how assertions from eduRoam and eduGAIN are handled and shared safely between different layers.

In this particular scenario user U, who has a valid digital identity at his home institution (HI), attempts to gain wireless network access as a guest at the visited institution. As the visited institution is the owner of the resource network it will be called Resource Institution (RI) from now on to preserve a common terminology with AAI. Both HI and RI are members of the network access federation. Furthermore, the user desires to obtain access to a web resource hosted at another RI in a different AAI (e.g. a different university) based on the successful network login.

The sequence of events and the required interactions involved in the process of granting U access to the network at RI-1 and access to the web resource provided by RI-2 are described in the Figure 2.2 below.

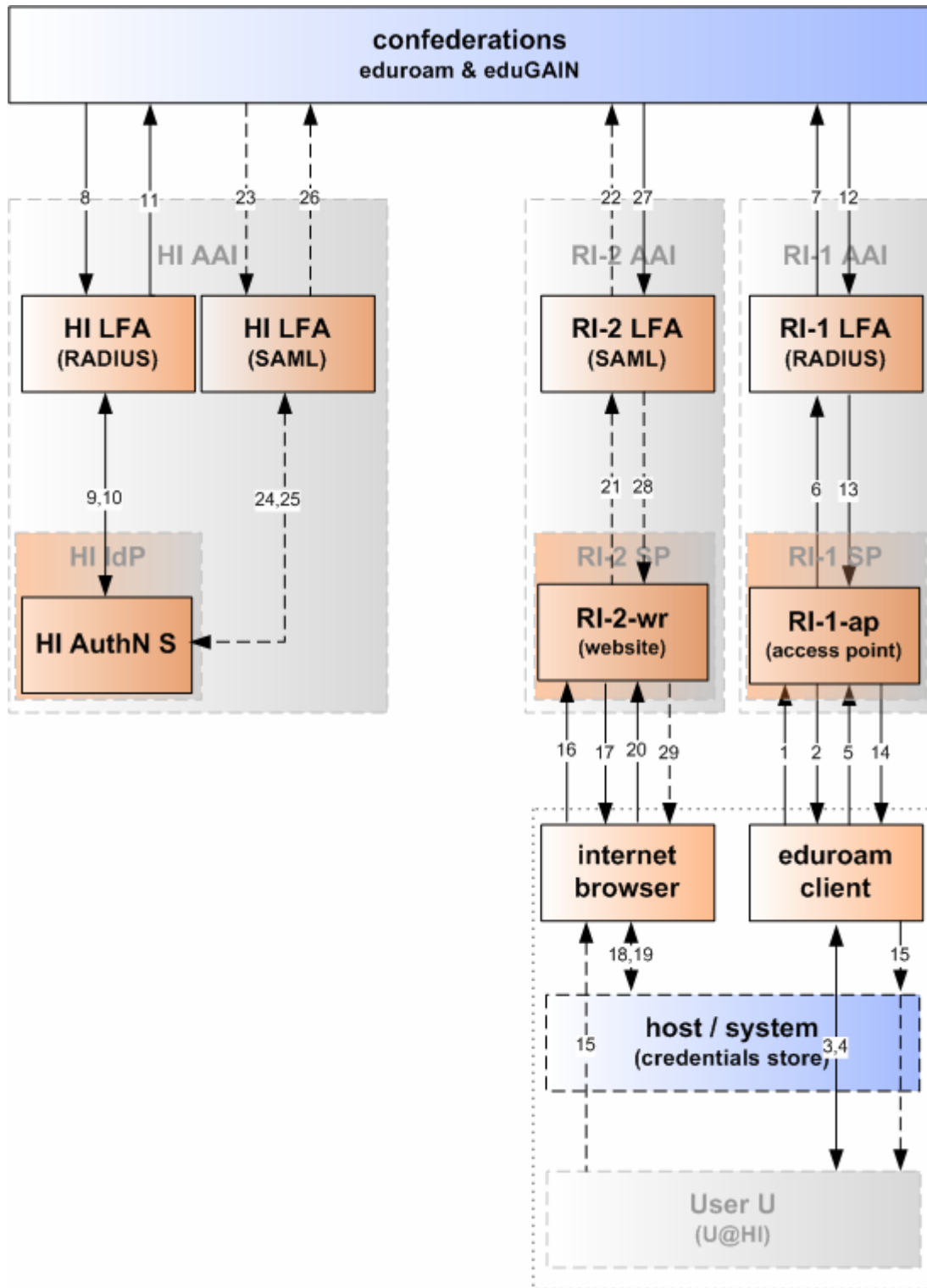


Figure 2.2: Communication pattern for network and web resource access at two different RIs

U tries to connect to a wireless network by using a network access client (e.g. WPA supplicant):

1. The client of U associates with the wireless network access point at RI-1-ap;
2. The access point considers this as a request for authorisation to use the network, and since U is not authenticated, U is asked for their user identity, unique within their home federation, and their encrypted identity credentials;
3. Depending on the type of client (supplicant) used, the credentials may be retrieved automatically from a local store or U may be prompted to select their credentials if these are not available;
4. (U enters or selects their credentials;)
5. The client encrypts the credentials, which can be decrypted by the Authentication Service at his HI only, as well as the digital identifier "<U@HI>", and sends them off to the access point;
6. The access point forwards the authentication request, the user identifier and the encrypted credentials to RI-1's Local Federation Adaptor (local authentication server, e.g. RADIUS);
7. The local authentication server, acknowledging the fact that it is not an authoritative authentication server for identities issued by the HI, forwards the request with the associated data to the confederation responsible for delivering the authentication request to the HI (eduroam);
8. The request is forwarded through the confederation to the HI LFA (RADIUS server);
9. The HI LFA passes on the request to the HI Authentication Service (HI AuthNS);
10. The HI AuthNS verifies the credentials and (after a positive result) sends back an authentication assertion;
11. The HI LFA forwards the assertion to the confederation;
12. The assertion is forwarded through the confederation to the RI-1 LFA;
13. The RI-1 LFA forwards it to the RP-1-ap, the access point;
14. The access point verifies the assertion and grants U access to the network.
15. The access point also forwards the assertion given out by HI AuthNS proving the identity of U, which is stored locally in a credentials store on the user's device. User U is informed that network access is granted, and in case they hadn't done so before they now open a web browser and enter the address of the desired web resource (RI-2-wr).
16. The internet browser tries to access the web resource RI-2-wr;
17. The web resource considers this as a request for authorisation to use the application, and since U is not yet authenticated at this resource, it asks for the user's identity or for proof of a previous authentication;
18. The internet browser requests an assertion that was provided during the network login;
19. The assertion is retrieved from the credentials store;
20. The Internet browser passes on the assertion to RI-2-wr.

In a basic scenario the SSO process could be completed at this point. However, depending on the authorization required for access to the resource, RI-2-wr may now issue requests for additional attributes for user U based on the authentication assertion, and/or grants U access to the application, which provides the actual content to the Internet browser. In the example of an additional attribute request towards the HI, the following steps could be added to the process:

21. The RI-2-wr forwards the attribute request containing a handle based on the previously obtained authentication assertion to the RI-2 LFA;
22. The RI-2 LFA forwards the request to the confederation responsible for identifying the user's home federation and delivering the assertions towards the HI (eduGAIN);
23. The request is forwarded through the confederation to the HI LFA;
24. The HI LFA passes on the request to the HI Authentication Service (HI AuthNS);
25. The HI AuthNS verifies the handle and (after a positive result) sends back an attribute statement containing the requested attributes;
26. The HI LFA forwards the attribute statement to the confederation;
27. The attribute statement is forwarded through the confederation to the RI-2 LFA;
28. The RI-2 LFA sends it to the RI-2-wr.
29. The RI-2-wr evaluates the attribute statement and decides whether to grant access to the user.

This single sign-on scenario is based on the assumption that the user has had previously no Internet access, and therefore authentication to the resource is based on the assertion obtained during the network access phase. Alternatively, other uSSO cases can be envisioned where the user is already logged into the network and the assertion is provided from a previous resource access, through an eduGAIN authentication procedure. This procedure would also have to be carried out in the case where no relevant assertion for RI-2-wr is available in step 19 (for instance if RI-1 and RI-2 are not connected through federated SSO). The corresponding sequence of events is similar to the one described in steps 21-29, with authentication request replacing the attribute request.

3 SSO Requirements

This section presents general requirements, which need to be fulfilled by the uSSO solution. As uSSO combines roaming and AAI, the requirements are a combination of:

- Roaming requirements
- AAI requirements
- Common/Integration requirements

Furthermore, since the uSSO activity doesn't start in a green fields environment, but instead builds on the already established infrastructures, i.e. eduroam and eduGAIN, a number of additional specific requirements arise from the architectural choices that have been made in order to build these infrastructures.

The requirements discussed here are based on the requirement classes defined in DJ5.2.1 "Documentation on AAI Requirements" and DJ5.1.2 "Documentation on GÉANT2 Roaming Requirements".

Most requirements are similar or the same for roaming and AAI; these have been indicated with CRx, where CR stands for "Common Requirement". Special roaming requirements are indicated with RRx and AAI requirements with ARx. There are no conflicts arising from the combination of roaming and AAI requirements.

3.1 Security Requirements

CR1: Reasonable security: The uSSO shall offer carefully chosen trust and enforcement levels in accordance with different application or service needs. The motivation to consider deploying an infrastructure with a lower trust level (if at all) is the possibility of offering solutions with improved usability and performance, combined with a lower security. The GÉANT2 uSSO shall provide a balance between security levels and usability and performance, always according to the nature of the protected resource in each case.

CR2: Data Integrity: The success of the federated uSSO depends completely on the preservation of data integrity as well as secure transfer and processing. Trust in the data integrity is essential for establishing the federation as such, and is also crucial to attract new members to federations. To ensure the integrity of security-related information, the data must be regularly refreshed; revocations of credentials should be agreed at intervals that do not impair usability and the security of the system, though aiming at a high performance, and must be able to accommodate support for multiple authentication methods.

CR3: Privacy Protection: To protect the users privacy and to follow the strict European and national regulations on privacy preservation, the infrastructure must avoid data leakage when performing AA interactions and provide users with means to have control over what information about them is exchanged and for what purpose.

CR4: Mutual authentication: In order to ensure the desired level of security, mutual authentication should take place between the end-user U and the authentication server.

CR5: Verifiability: The very nature of authentication and authorisation requires keeping a clear and uniform end-to-end record of relevant data related to service access. The infrastructure shall provide the necessary means to retrieve this information when appropriate evidence about a certain interaction is requested.

3.2 Standards Compliance and Integration

CR6: Openness: Building blocks and service elements of the infrastructure shall use open standard protocols and mechanisms to interconnect with other elements, either internal or external.

RR1: Integration: The Local Federation Adaptors (LFA) of eduroam are currently based on 802.1X and RADIUS technology. It should be possible to integrate other technologies (evaluated in JRA5 work item 4). eduroam should also be applicable to wired Ethernet "docking points" at visited institutions, that means 802.1X and the RADIUS infrastructure could be used for fixed network access as well.

AR1: Integration: AA solutions are already, partially or fully, in place at a number of NRENs, universities and other higher education institutions with various applications using them for access control to resources or services. As a result, user communities and well-defined operating procedures exist. The GÉANT2 AAI must be able to offer integration of existing AA solutions or infrastructures at the appropriate trust level in the trust fabric. In order to do so JRA5 shall offer alternative migration or integration strategies, exploiting for example the possibilities of providing a gateway functionality to convert different federation protocols (e.g. SAML1/SAML2/WSF) to extend AA capabilities across federations and domains.

AR2: Neutrality: Since the infrastructure is aimed at incorporating different existing systems and will be used in a number of application domains, it is necessary not to mandate specific technologies at the edges of the infrastructure. This is because it could create problems in integrating local infrastructures and adapting applications willing to use it. Open and general interfaces shall be provided both internally (to connect local AA components) and externally (to connect applications).

3.3 Operational Requirements

CR7: Scalability: The infrastructure shall be able to grow in several dimensions: regional – spanning many countries/domains; functionally – spanning many applications and services; structurally – reaching high integration with other regions/domains and reaching every end user/service.

CR8: Ease of use: It is a basic requirement for any middleware infrastructure to be as seamless as possible. This means that the AAI shall impose a minimum burden on end users and on administrators of services. No additional work shall be put on operators of authentication services or on the staff defining and controlling the access policies to a certain set of resources.

CR9: Robustness: The infrastructures that form the basis of uSSO, eduGAIN and eduroam, are a critical resource for any networked application. This implies that the infrastructure must be able to handle the expected load on the system.

CR10: Flexibility: The infrastructure shall allow each of the actors interacting and/or using it to manage and enforce their own policies. This includes authenticators and identity providers, service providers, user communities, etc. The basic principles of federated administration are to be applied here, allowing for the decoupling of AA procedures by means of the establishment of a web of trust among the actors.

3.4 Organisational Requirements

CR11: Federation service provider: One institution shall be appointed to be the ‘federation service provider’ for every single federation. This institution shall be responsible of the administration and operation of a Local Federation Adaptor (LFA) in charge of connecting local AA and roaming solutions to the confederation infrastructure.

CR12: Federation Agreement: For each federation there should exist an agreement specifying the purpose, the technical and business terms of the federation. This agreement should provide members of the federation and other relying parties with sufficient information on which to base their level of trust in the federation service.

CR13: Availability of the federation Agreement: All members of the confederation providing uSSO should be able to access the information contained in the federation agreements of other participants in the confederation. This should allow them to obtain sufficient information on which to base their level of trust in the services provided by the other participant federations. An English version of the agreement should therefore be available for each federation.

3.5 Authentication and Authorisation Mechanisms

CR14: Home Institution choice of authentication mechanism: There are a number of authentication mechanisms available and in use today; the decision of which one to choose and to provide to the user (dependent on the respective scenario) shall be made by the HI. The security level for this mechanism **MUST** be in conformance with the requirements for qualifying as a member of the confederation (to be specified in the confederation policy). The level of trust allocated to an asserted identity is to be based not only on the authentication mechanism used, but also on the Identity Management practices within the federation.

CR15: Remote Institution autonomy: The RI may decide not to trust specific authentication methods used by the HI, and consequently block all authentication attempts when a method that is considered unsafe is used.

RR2: User ID format: The U@HI presentation should be in the normal DNS format user@domain.tld. Internationalised Domain Names (IDN) can be used.

AR3: Harmonized user identity model: Although the choice of authentication mechanisms to be used locally belongs to each HI, a harmonized identity model should be agreed upon in order to ease communication across the different federations. The scope of the user identifier is the confederation. Mapping between the used attributes should be possible and the model should involve the same minimal choice of attributes.

CR16: Credential protection: Credentials shall not be visible in a readable form by any component other than by the user's own HI or by trusted authentication software. The HI may however release other attributes of the user in accordance with the governing policies.

AR4: Level of Assurance (LoA): The participant AAls should be able to handle authorisation models supporting different levels/classes of access rights.

4 Conclusions

The presentation of the uSSO Problem and the typical usage scenario result in the adjacency to roaming and AAI becoming obvious. Hence the requirements presented for uSSO largely comprise the requirements for eduroam and eduGAIN, and augment these to some degree.

Whereas eduroam and eduGAIN already offer a comfortable architectural basis to build a federated solution for network and service access, the desired combination of these two systems poses as well the biggest challenge. Many of the various requirements specified, especially those considering the organisation of the uSSO participants, are already met when implementing one of these two systems. The formulation of the uSSO requirements and possible scenarios based on the experience accumulated with roaming and AAI constitutes an important step towards defining an architectural solution for uSSO. The first results of the DAME subproject will be used for the evaluation of alternative models and so significantly aid developing and describing in detail the architectural model in the next SSO deliverable.

It is difficult to predict the evolution and results of this work item in JRA5 by now. All further developments for uSSO will thus need to be based on and conform to the requirements defined in this document.

As work progresses a unified testbed will be built, using the results from eduroam and eduGAIN. Therefore, an important prerequisite is having an operational eduGAIN infrastructure, which is currently developed in the JRA5 work item 2.

5 References

- [DJ5.1.1] Roaming Glossary of Terms
<http://www.geant2.net/upload/pdf/GN2-04-111Final.pdf>
- [DJ5.1.2] Documentation on GÉANT2 Roaming Requirements
<http://www.geant2.net/upload/pdf/GN2-05-71v6.pdf>
- [DJ5.2.1] Documentation on GÉANT2 AAI Requirements
<http://www.geant2.net/upload/pdf/GN2-05-026v6.pdf>

6 Acronyms

In JRA5 used acronyms can be found in the JRA5 Glossary of Terms [DJ5.1.1]. Additional terms are listed below.

[DAMe]	Deployment of Authorisation Mechanisms for federated services in eduroam, a JRA5 subproject
[LFA]	Local Federation Adaptor
[LoA]	Level of Assurance – describes the degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity.
[WSF]	Web Services Framework
[IdM]	Identity Management – the management of the identity life cycle of entities (subjects or objects), including establishment, description and destruction of an identity.