Best practices for managing authorisation

Published Date:	13-06-2017
Revision:	1.0
Work Package:	JRA1
Document Code:	AARC-JRA1.4E
Document URL:	https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4E.pdf

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Table of Contents

Table of Figures

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

1 Introduction

Once a user is authenticated, resource access is granted by authorisation policies enforced by service providers (SPs). National identity federations and eduGAIN, through identity providers (IdPs), provide a well-established authentication service for a home organisation's (HO) users. However, nowadays, research collaborations (RCs) are composed of members belonging to different federations. An RC usually relies on digital resources and services both to do research work and to communicate and manage the collaboration itself, but it is the RC that is responsible for defining the access rights to its resources. Therefore, authentication and authorisation processes for resource access are very important for RCs.

Authorisation policy enforcement always happens on SPs (even though not always on just the resource SP alone, e.g. in the case of an IdP/SP proxy). When an SP has all the information to build a consistent authorisation policy for each user, this is not a problem. However, there are several cases where this is not possible or desirable, especially when RCs are involved. SP-managed authorisation, or application-based authorisation, can face issues related to (multiple) source of authority, scalability, and RCs interaction.

HO IdPs may be used as an authoritative source of information for determining resource access. A common example is the "common-lib-terms" entitlement, which is used by many institutions to signal to a publisher that the user is authorised to access the SP resources (and that the institution will pay for its use).

As already stated, in the case of RCs there is not just one HO on which to rely for authoritative information.

SPs cannot easily collect information to manage different access rights for thousands of users, and often the IdPs of R&E entities such as universities deal with tens of thousands of users.

A user may be a member of many RCs, and it is impractical for an institution to manage RC-specific entitlement information on a per-user basis. A more practical approach for RCs is to create a virtual organisation (VO) and to manage its entitlements itself. The information on which authorisation policies rely can then be collected using an attribute management system and its information exposed via attribute authorities (AAs).

2 Authorization information sources

As noted above, while authorisation policy enforcement takes place at the SP, the information that needs to be evaluated by those policies, usually attributes and roles, will often need to be sourced from different providers. Two such authorisation information sources are considered below: identity providers and attribute authorities.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

2.1 Identity Providers as authorisation information source

When IdPs are used as the source of information for authorisation purposes, user information is encapsulated in attributes and transmitted to SPs along with the authentication assertion, as shown in Figure 2.1.

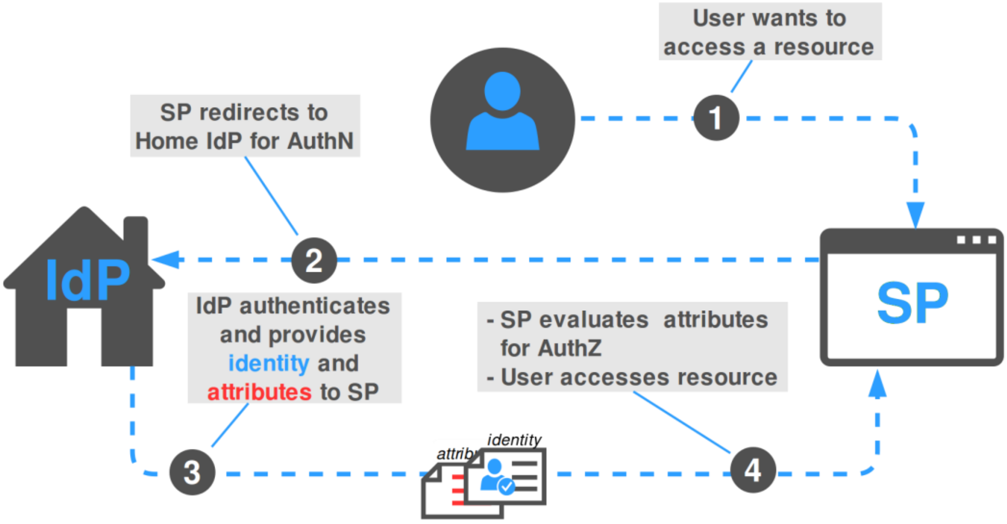
User wants to access a resource
1
SP redirects to Home IdP for AuthN
2
IdP
SP
IdP authenticates and provides identity and attributes to SP
3
- SP evaluates attributes for AuthZ
- User accesses resource
4
identity
attrib

Figure 2.1: IdP as AuthZ source: SPs leverages attributes coming from IdP.

2.2 Attribute Authorities as authorisation information source

AAs can store additional user attributes[1] including, but not limited to, group membership, virtual organisation (VO) affiliation and/or role.

In SAML authentication flows, AAs do not participate in the authentication process, so to use them as a source they have to be queried directly. Typically, the user identifier from the authentication is leveraged as a user identifier to retrieve the additional attributes at the AA.

Depending on who queries the AA and at what time, three general models can be outlined. Each of these is described below.

[1] Many virtual organisations also issue an extra identifier for the user.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

2.2.1 Identity Provider

The HO IdP can collect additional attributes from AAs with the SAML attribute query, or by employing custom connectors available on the AA (if the AA is managed by the home organisation IdP, direct database/directory queries are often employed). In this model (Figure 2.2), the IdP will aggregate all the attributes and push them to the SP, so that the SP does not need to be aware of the existence of the AA.

Importantly, this model is not suitable for RCs: it would require too great a coordination effort to have all the RC members' HO IdPs query a common AA, aggregate the attributes, and finally release them to the SP(s) used by the RC.

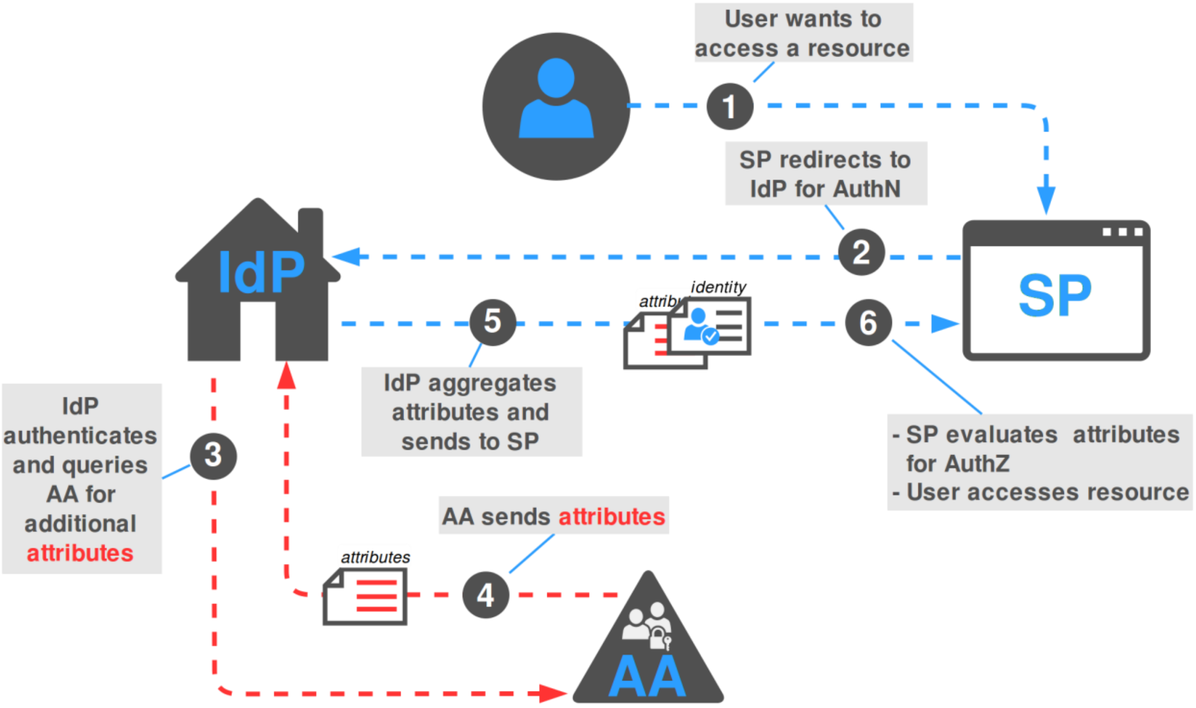
User wants to access a resource
1
SP redirects to IdP for AuthN
2
IdP
SP
5
attrib
identity
6
IdP aggregates attributes and sends to SP
- SP evaluates attributes for AuthZ
- User accesses resource
IdP authenticates and queries AA for additional attributes
3
AA sends attributes
attributes
4
AA

Figure 2.2: AA as AuthZ source for IdP: IdP aggregates AA attributes and pushes them to SP.

2.2.2 Service Provider

In this model (Figure 2.3), SPs are aware of the existence of an AA that has to be queried to retrieve attributes useful for the enforcement of the authorisation policies.

In the SAML world, SPs use the SAML attribute query to pull the additional attributes after receiving the authentication assertion from the IdP along with a user identifier. In order to query the AA, the SAML attribute query must contain a user identifier linked to the user's attributes.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

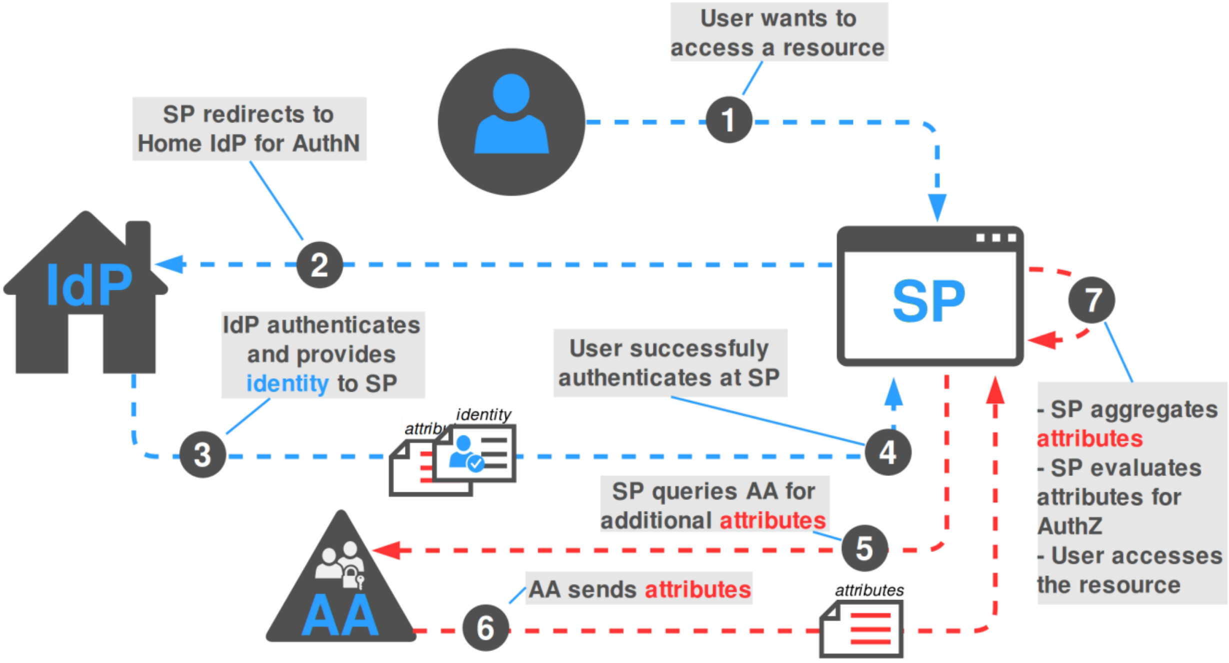
User wants to access a resource
1
SP redirects to Home IdP for AuthN
2
IdP
SP
7
IdP authenticates and provides identity to SP
3
identity
attrib
User successfully authenticates at SP
4
SP queries AA for additional attributes
5
AA
AA sends attributes
6
attributes
- SP aggregates attributes
- SP evaluates attributes for AuthZ
- User accesses the resource

Figure 2.3: AA as AuthZ source for SP: SP queries AA for attributes.

2.2.3 IdP/SP Proxy

IdP/SP proxies sit in between the IdP, which performs the authentication, and the SP that will receive the authentication assertion and the user attributes. Proxies with attribute aggregation and external attribute query features can thus modify the attributes set that is part of the authentication flow. Additional attributes, which will eventually be used by the SP to enforce the authorisation policies, can be retrieved from AAs and aggregated into the original set.

In this model (Figure 2.4), the attributes coming from the IdP and the AA are pushed to the SP. Neither the IdP nor the SP needs to be aware of the existence of the AA, but they both should have a trust relationship with the proxy.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

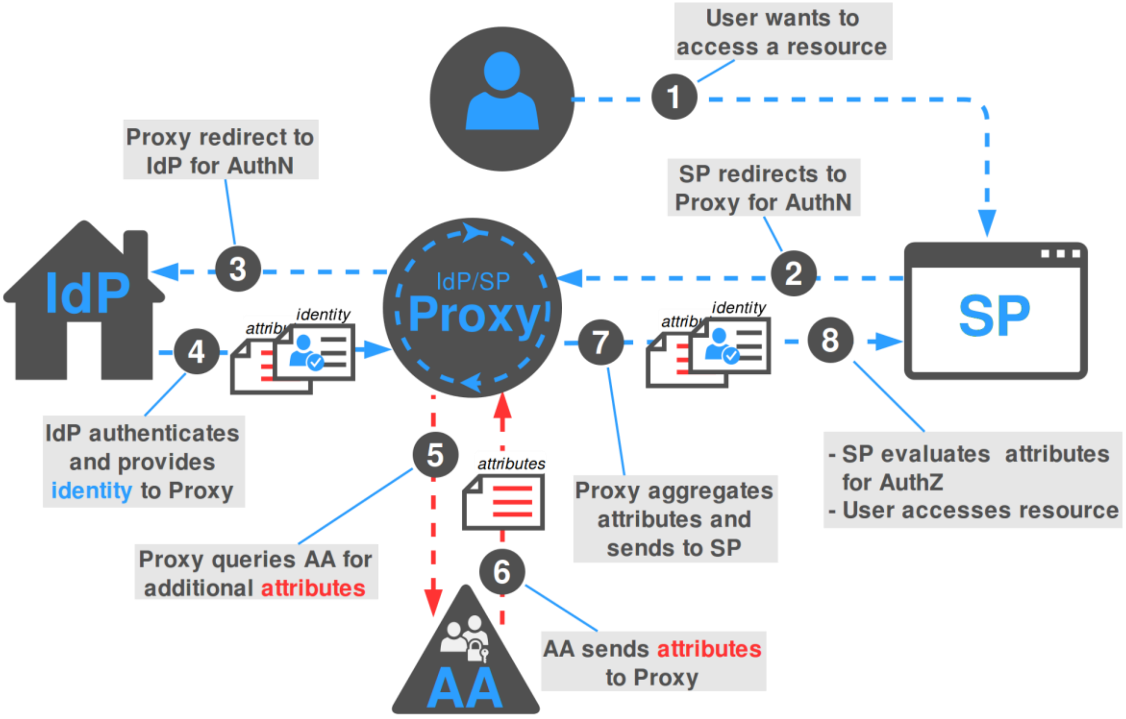
User wants to access a resource
1
SP redirects to Proxy for AuthN
2
Proxy redirect to IdP for AuthN
3
IdP
IdP/SP
Proxy
SP
4
identity
attrib
IdP authenticates and provides identity to Proxy
5
attributes
Proxy queries AA for additional attributes
6
AA
AA sends attributes to Proxy
7
Proxy aggregates attributes and sends to SP
8
- SP evaluates attributes for AuthZ
- User accesses resource

Figure 2.4: AA as AuthZ source for IdP/SP Proxy: proxy aggregates AA attributes.

3 Authorisation attributes

This section considers three types of information that can be used for authorisation: affiliation, entitlement and level of assurance.

3.1 A basic example: affiliation as authorization data

In a simple scenario, affiliation information, usually released by IdPs, can be used for authorisation. In the context of the SAML 2.0 protocol and its use in eduGAIN, this information is transmitted employing eduPersonAffiliation (ePA) [I2-EPA] or eduPersonScopedAffiliation (ePSA) [I2-EPSA], and preferably the latter.

It is important to understand that affiliation can be authoritatively asserted only by the organisation to which the user belongs, the so-called home organisation.

Table 3.1 below shows a practical example of how to use ePSA to enforce authorisation policies, taking an SP that has two service levels: base and advanced. To qualify for each service, ePSA attribute values are evaluated at login time. In the example shown below, not all the values of ePSA let the user access the protected, advanced services and, as a minimum, the member affiliation is needed to successfully log in.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Best practices for managing authorisation

User ePSA values	Policy		
	Login	Base Service	Advanced Service
`affiliate@foo.bar`	NO	N/A	N/A

`member@foo.bar,`
`student@foo.bar`
	YES	YES	NO

`member@foo.bar,`
`staff@foo.bar`
	YES	YES	YES

`member@foo.bar,`
`faculty@foo.bar`
	YES	YES	YES

Table 3.1: Affiliation as authorization data.

It is worth mentioning that affiliation, as defined in the eduPerson schema for the attribute ePSA [I2-EP], carries some role information also, but in a very broad and general sense. In the context of research collaborations, affiliation can be used for coarse-grained authorisation management. When resource access is based on more fine-grained authorisation policies, entitlements (see Section 3.2 below) should be preferred.

3.2 Entitlements

Entitlements indicate a set of rights to specific resources. In SAML 2.0/eduGAIN, entitlements are stored in the attribute eduPersonEntitlement (ePE) [I2-EPE]. Entitlements can be information targeted on either the resource, or on the user's groups membership and roles.

In the first case, entitlements can represent the specific right of a user to access a resource. In sensitive research fields, such as biomedicine, access to data is subject to approval, and permission to access the data can be conveyed through one or more entitlements.

When group- and role-based access control policies are needed, the membership information can be transmitted with the attributes ePE, or isMemberOf.

Being a URI, eduPersonEntitlement can be used for fine-grained representation and transmission of a variety of information, including groups membership, roles, and scope.

Table 3.2 below shows an example of how to use ePE to enforce authorisation policies, taking an SP that has two access levels: user and manager.

User ePE values	Policy	
	User access	Manager access
`urn:mace:<namespace>:<authority>:group:vo.example.org`	YES	NO
`urn:mace:<namespace>:<authority>:group:vo.example.org:role=manager`	YES	YES

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Table 3.2: eduPersonEntitlement as authorization attribute for groups and roles.

Entitlements are suitable for conveying authorisation information for research collaborations and VOs.

A standardisation effort regarding the use of entitlements to best represent groups membership and roles has been carried out within AARC [AARC-JRA1.4A]. AARC2 will address more advanced scenarios related to distributed authorisation.

3.3 Level of Assurance

The authorisation process can also be related to the level of assurance (LoA). Assurance information can be transmitted leveraging attributes, such as eduPersonAssurance [I2-ePAs], and the SAML authentication context class.

While some identity federations[2] and e-infrastructures[3] have deployed their own LoA scheme, the REFEDS Assurance Working Group and AARC are working to define common LoA recommendations [REFEDS-AWG]

4 Additional Considerations

This section addresses three further considerations relating to authorisation management: trust relationships, delegated authorisation management, and authorisation attributes and token translation.

4.1 Trust relationships

In some of the models related to using attribute authorities as the authorisation information source, the trust relationships among all the components are heavily dependent on the architecture and the attributes flow. Another important factor to consider is the ownership of each component, since it can reshape the circle of trust (for example, if the AA is owned by the same home organisation that owns the IdP).

In the case of using an AA as the authorisation source for an SP, all the trust relationships should be considered direct, as shown in Figure 4.1. For IdP to SP and AA to SP, the nature of the trust relationships is

[2] Many eduGAIN identity federations have defined their own LoAs. As an example, see the SURFnet LoAs [SURF-LOA].

[3] EGI is an example of an e-infrastructure that has defined its own LoAs for authorisation purposes. See [EGI-LoA].

apparent, since they need to exchange information. The trust relationship between the IdP and the AA is also shown as direct, since the AA should be linked to the IdP with a shared user identifier.

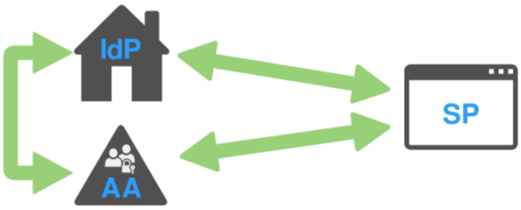

Figure 4.1: Trust relationships for AA as AuthZ source for SP.

In the case of using an AA as the authorisation source for an IdP/SP proxy, the trust relationships between the IdP/SP proxy and all the other components are direct, but those between the SP on one side and the IdP and the AA on the other are indirect, as shown in Figure 4.2. In theory, because of the proxy-based attributes flows, the SP does not need to be aware of the existence of the AA, or even of the home organisation IdP that has originally authenticated the user. In real life, trust relationships between the HO IdP and the SP often pre-exist, either because the SP services are contract-based, or because they are both connected through a national identity federation or through the eduGAIN inter-federation service.

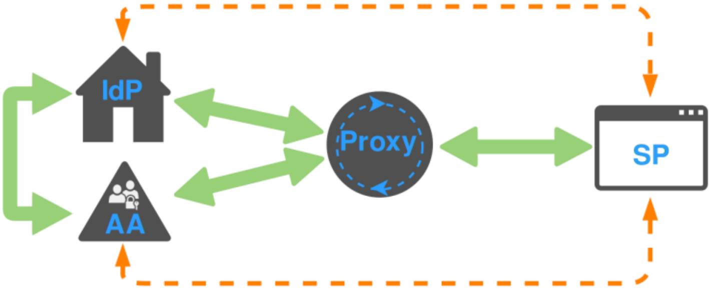

Figure 4.2: Trust relationships for AA as AuthZ source for IdP/SP Proxy.

4.2 Delegated authorisation management

In the context of research collaborations, it is necessary, or at least desirable, to delegate the management of the resource authorisation entitlements to people who are not the direct resource owners. This is a very common scenario in RCs. An RC typically has a VO/group management system in which the members of the collaboration are assigned to groups and/or roles. Access to the resources is typically granted based on the group(s) that the user belongs to in the collaboration, and/or based on the role(s) (s)he holds. In small collaborations, with a small number of members and resources, authorisation management can happen centrally. In larger collaborations, the internal structure of the collaboration is much more complicated and this might require the group/role membership management to be distributed and delegated as needed, to map the collaboration structure.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

4.3 Authorisation attributes and token translation

Token translation services can be used to connect IdPs and SPs that employ different authentication protocols, but while syntactic and semantic differences among protocols can be addressed, the differences in context reference are more difficult to overcome.

In a scenario where SAML 2.0/eduGAIN is the destination authentication protocols/context reference and OIDC/Google is the source reference, some attributes and concepts will not be available at the origin, so they will not be available at the destination. Examples of attributes that cannot be easily translated are:

- Affiliation.
- Entitlements.

To overcome this issue, proxies with attribute aggregation and external attribute query features can leverage AAs to collect additional attributes to be used as authorisation entitlements.

The research leading to these results has received funding from the European Community’s Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

5 References

[AARC-JRA1.4A] Guidelines on expressing group membership and role information
https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4A.pdf

[EGI-LOA] EGI wiki page: AAI guide for SPs – Level of Assurance
https://wiki.egi.eu/wiki/AAI_guide_for_SPs#Level_of_Assurance

[I2-EP] eduPerson Object Class Specification
http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html

[I2-EPA] eduPersonAffiliation description
http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html#eduPersonAffiliation

[I2-EPAs] eduPersonAssurance description
http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html#eduPersonAssurance

[I2-EPE] eduPersonEntitlement description
http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html#eduPersonEntitlement

[I2-EPSA] eduPersonScopedAffiliation description
http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html#eduPersonScopedAffiliation

[REFEDS-AWG] REFEDS wiki page: Assurance Working Group
https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group

[SURF-LOA] SURFnet wiki page: Connecting your SP to SURFconext Strong Authentication
https://wiki.surfnet.nl/display/surfconextdev/Connecting+your+SP+to+SURFconext+Strong+Authentication

6 Glossary

AA	Attribute Authority
AAI	Authentication and Authorisation Infrastructure
AuthN	Authentication
AuthZ	Authorisation
HO	Home Organization
IdP	Identity Provider
LoA	Level of Assurance
OIDC	OpenID Connect
RC	Research Collaboration
REFEDS	Research and Education FEDerations group
R&S	Research and Scolarship
SAML	Security Assertion Markup Language

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

SP	Service Provider
URI	Uniform Resource Identifier
VO	Virtual Organization

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).