A specification for providing information about an end service to a Discovery Service

Publication Date	2022-04-11
Authors:	Marcus Hardt (ed.), Valeria Ardizzone, Jens Jensen, Ivan Kanakarakis, Christos Kanellopoulos, Nicolas Liampotis, Mikael Linden, Mischa Sallé
Document Code:	AARC-G063
DOI:	10.5281/zenodo.6938616
Reference as:	https://aarc-community.org/guidelines/aarc-g063
Community:	Architecture Area

Abstract

This specification defines how SP-IdP Proxies can provide hints about services towards Discovery Services to improve the user experience of the authentication process.

Status of this document

This specification defines a hint parameter to improve the user authentication flow. The parameter specified in this document is defined in a similar context as the other hint parameters (`aarc_idp_hint` [AARC-G061] and `aarc_ds_hint` [AARC-G062])

A list of all AARC community guidelines and the latest revision of each guideline can be found at https://aarc-community.org/guidelines.

1. Introduction

In the AARC Blueprint Architecture (BPA) [AARC-G045], the service that the user tries to access is usually not directly connected to the authenticating IdP (i.e. the IdP identifying the user as in [SAML2Core Sec. 3.4.1.5]), but the connection is established through one or more upstream SP-IdP-proxies. The appropriate IdP needs to be chosen by users at the Discovery Service of those SP-IdP-proxies (Figure 1). Such a discovery service can be integrated with the proxy, or be a centrally provided one (e.g. Seamless Access). The authentication flow may include the Infrastructure Proxy and the Community AAI as shown in Figure 2.

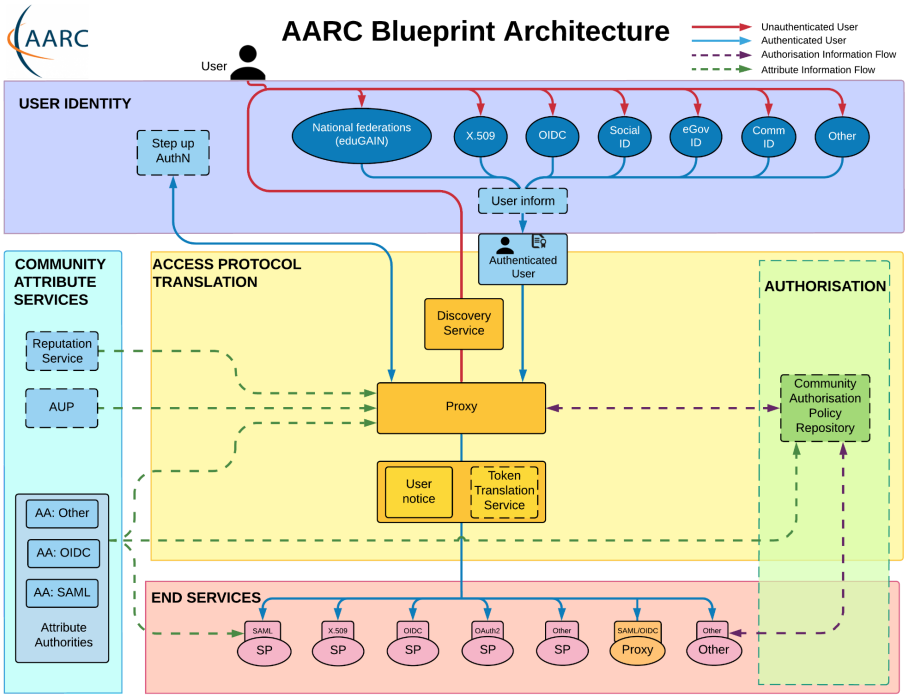

Figure 1: The AARC Blueprint Architecture. A proxy has a Discovery Service attached to it.

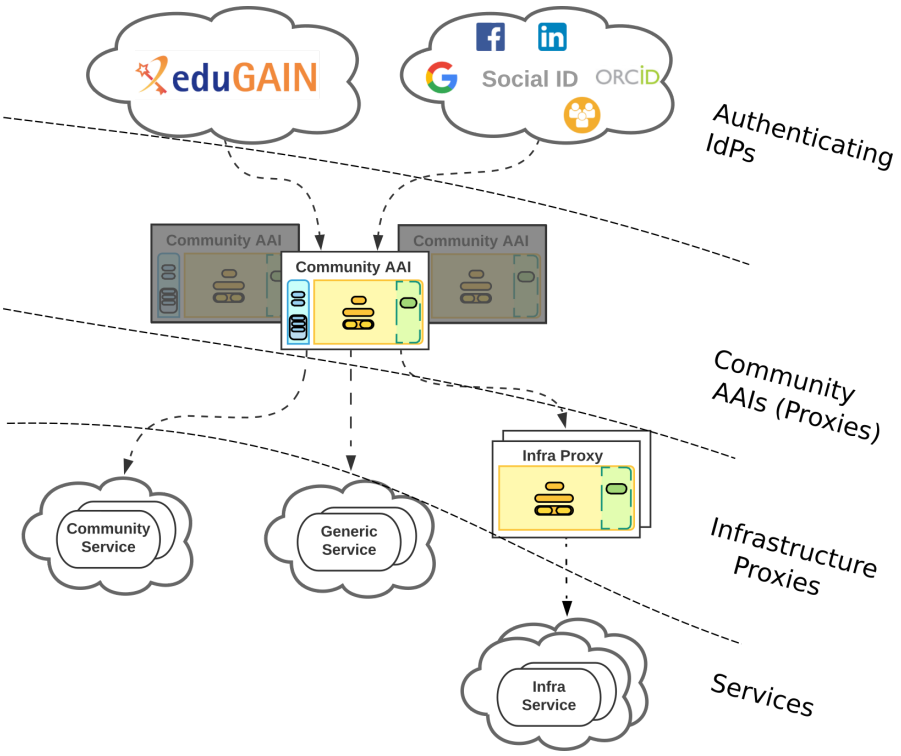

Figure 2: Different entity types shown in the Blueprint Architectures 2019 diagram [AARC-G045].

Discovery protocols, typically used in federated environments lack a standardised mechanism to let an IdP provide information about an end service “S” to a Discovery Service (see OASIS "Identity Provider Discovery Service Protocol and Profile" [IDPDSP]). This is problematic when SP-IdP-Proxies are involved, since this creates confusion to which service a user would authenticate.

This document defines a generic web-browser based way to provide this information in the form of hints. Valid values of these hints - i.e. the service identifiers - are agreed between the hint producer and the hint consumer and are communicated out of band to the hint producers.

This enables SP-IdP-Proxies to provide information to Discovery Services about the service that a user is trying to access. Lacking such information causes a suboptimal user experience at the Discovery Service.

In the context of this document we only consider the use case of enabling Discovery Services to better guide the user. However, the use of this specification is not limited to only such a purpose.

1.1. Definitions

Whenever we use the term "Identity Provider" (or "IdP") we refer to what SAML calls IdPs and OpenID calls OpenID Connect Providers (OPs). Similarly, when we use the term "Service Provider" (or "SP"), we refer to what SAML calls SPs and OpenID Connect calls Relying Parties (RPs).

This document defines the following terms:

- A "service identifier" identifies an entity, which could generally be an SP, an authenticating IdP, an SP-IdP-Proxy[AARC-G045] or a Discovery Service. Within the scope of this document, this identifier refers to either an SP or a collection of SPs that can be treated by the Discovery Service as a single SP.
- A "hint producer" produces and sends hints. In the scope of this document, this is an SP-IdP-Proxy.
- A "hint consumer" receives and consumes hints. In the scope of this document, this is the Discovery Service of the SP-IdP-Proxy that produced the hint.

This document also uses the following terms (see also Fig.1 above):

- An “SP-IdP-Proxy” [AARC-G045] is a bridge or gateway between a set of IdPs and a set of SPs.
- A “Discovery Service” (DS) [IDPDSP] is the logical element providing the user with a list of IdPs to choose from. It can be integrated into other services or SP-IdP-proxies, allowing users to choose an IdP for authentication.
- The “authenticating IdP” is the IdP at the end of the authentication chain at which the user ultimately identifies. In the AARC BPA [AARC-G045], the authentication chain typically contains one or more intermediate SP-IdP-proxies ([SAML2Core] sec. 3.4.1.5).
- “Community AAIs” [AARC-G045] serve as IdPs or SP-IdP-Proxies for specific communities.
- “Infrastructure Proxies” [AARC-G045] are used to connect all services of a specific infrastructure. Infrastructure Proxies may be connected to multiple Community AAIs.

1.2. Use Case

To illustrate the benefit that the specified hint provides, we describe the authentication flow that a user takes when coming from a Service Provider “S” connected to an SP-IdP Proxy “P” with a Discovery Service “DS”:

1. User visits a Service Provider S with a web browser.
2. S redirects the user to its SP-IdP Proxy P.
3. P redirects the user to its Discovery Service DS where the user must choose an IdP to authenticate with.
    - DS may show the user information about the end service S that requested the authentication.
    - DS may alter the selection or presentation of IdPs presented to the user based on the information about the end service and other information available to it. For example, it may remove IdPs with a too low level of assurance, or highlight a default.
4. User is redirected to the chosen IdP
5. After successful authentication, the user is redirected back to P where it may be shown which attributes are going to be released to the Service S.
6. The user is redirected to the Service Provider S.

1.3. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Context

This specification focuses on web-SSO-based flows, so will reference HTTP commands like GET and POST, but it does not exclude non-web-browser based flows, nor does it exclude other protocols.

3. Specification

The hint parameter specified in this document is the **`aarc_service_hint`**: a hint that allows its producer to provide information about the originating SP, consumed by a DS (i.e. the hint consumer).

The following rules apply to this parameter:

1. The hint consumer MUST be capable of processing the hint parameter in GET requests.
2. The hint consumer SHOULD be capable of processing the hint parameter in POST requests.
3. A hint consumer MAY ignore all or part of the value of a received hint parameter.
4. The value of the `aarc_service_hint` hint MUST be a single URL-encoded service identifier with the following additional rules:
    a. Forward slashes ('/') MUST be percent-encoded ([RFC3986] section-2.1]).
    b. Case sensitivity of the encoded value MUST follow the underlying specification of the original unencoded value.
5.
    a. The service identifier itself MUST allow the hint consumer to identify the SP (which can either be a single SP or a collection of SPs that can be treated by that hint consumer as a single SP).
    b. This document does not make any assumptions on the actual service identifiers of the hints. Valid values - i.e. the service identifiers - MUST BE agreed upon between the hint consumers and hint producers.

References

[AARC-G045] AARC Blueprint Architecture-2019
https://aarc-project.eu/guidelines/aarc-g045

[AARC-G061] A specification for IdP hinting
https://aarc-community.org/guidelines/aarc-g061

[AARC-G062] A specification for hinting an IdP which discovery service to use
https://aarc-community.org/guidelines/aarc-g062

[IDPDSP] OASIS Identity Provider Discovery Service Protocol and Profile
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.html

[RFC2119] Key words for use in RFCs to indicate Requirement levels
https://tools.ietf.org/html/rfc2119

[RFC3986] Uniform Resource Identifier (URI): Generic Syntax
https://tools.ietf.org/html/rfc3986

[SAML2Core] SAML2-Core-OS §3.4.1.2 and §3.4.1.3
http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

Appendix A: Example

A proxy produces a hint to provide information about a connected Service Provider (identified as `urn:mace:kuleuven.be`) to a Discovery Service (identified as `https://disco.org`). The URL to which the proxy would redirect the user for the discovery is then:

```
https://disco.org/?<REQUESTPARAMS>
      &aarc_service_hint=$(urlencode(urn:mace:kuleuven.be))
```