SIR2

Federation Operator Practice: Metadata Registration Practice Statement

Autores	Jose Manuel Macías[1]
Última modificación	marzo 2016
Versión	1.0

This document is published under a Creative Commons Attribution-ShareAlike 3.0 Unported license.

[1] This document is based on the *Metadata Registration Practice Statement* for the SIR federation, by Ajay Daryanani Arjandas: https://www.rediris.es/sir/edugain/SIR_MRPS.pdf

Index

1. Definitions and Terminology

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].

The following definitions are used in this document:

Attribute	A piece of information describing the End User, his/her properties or roles in an Organization.
Attribute Authority	An organization responsible for managing additional Attributes for an End User of a Home Organization.
Authentication	Process of proving the identity of a previously registered End User.
Authorization	Process of granting or denying access rights to a service for an authenticated End User.
Digital Identity	A set of information that is attributable to an End User. Digital identity consists of Attributes. It is issued and managed by a Home Organization and zero or more Attribute Authorities on the basis of the identification of the End User.
End User	Any natural person affiliated to a Home Organization, e.g. as an employee, researcher or student making use of the service of a Service Provider.
Federation	Identity federation. An association of organizations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Operator	Organization providing Infrastructure for Authentication and Authorization to Federation Members.
Federation Member	An organization that has joined the Federation by agreeing to be bound by the Federation Policy in writing. Within the federation framework, a Federation Member can act as a Home Organization and/or a Service Provider and/or an Attribute Authority.
Home Organization	The organization with which an End User is affiliated. It is responsible for authenticating the End User and managing End Users' digital identity data.
Identity Management	Process of issuing and managing end users' digital identities.
Interfederation	Voluntary collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access Service Providers in another Identity Federation.
Service Provider	An organization that is responsible for offering the End User the service he or she desires to use. Service Providers may rely on the authentication outcome and attributes that Home Organizations and Attribute Authorities assert for its End Users.

2. Introduction and applicability

This document describes the metadata registration practices of the Federation Operator, as described in the Policy Document of the SIR2 federation, with effect from the publication date shown on the cover sheet. All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.

This document SHALL be published on the federation website at: https://www.rediris.es/sir2/federacion/politica, and describes the Metadata Registration Practice for the SIR2 federation.

The document supersedes the Metadata Registration Practice of the SIR Federation, described at https://www.rediris.es/sir/edugain/SIR_MRPS.pdf.

Both federations follow the “hub&spoke” federation paradigm.

The transition from the SIR federation to the SIR2 federation will imply the following:

- The Registration Authority will be kept the same, that is: http://www.rediris.es. The Federation Operator of both federations is RedIRIS.
- Registered entityIDs corresponding to identity providers in the SIR federation will keep the same values in the SIR2 federation, and will correspond with the same organizations. These will only be registered in the SIR2 federation after they agree with the new federation policy.
- End-points for the published entityIDs will reflect the new end-points in the SIR2 federation; this change will be reflected only in new metadata aggregates for the SIR2 federation. End-points in the SIR1 federation will continue to work during a period of time enough to transition to the new federation.
- New metadata set aggregates will be published under a new URL: https://md.sir2.rediris.es/, and using a new certificate, different to that of the SIR federation.
- SPs transitioning from SIR to SIR2 will have to comply with the new policy as well, prior to be registered in the SIR2 federation.

An entity that does not include a reference to a registration policy MUST be assumed to have been registered under an historic, undocumented registration practice regime. Requests to reevaluate a given entity against a current MRPS MAY be made to the federation helpdesk[2].

[2] Contacting SIR2 team: https://www.rediris.es/sir2/contacto

3. Member Eligibility and Ownership

The procedure for becoming a member of the Federation is documented at:

http://www.rediris.es/sir2/federacion/requisitos/

The membership process verifies that the prospective member has legal capacity, and requires that all members enter into a contractual relationship with the Federation Operator by agreeing to the Federation policy.

The membership process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the organization in dealings with the Federation Operator. Verification is achieved by personal contact between the Federation Operator and the organization; exceptionally via email or phone.

The process also establishes a canonical name for the Federation member. The canonical name of a member MAY change during the membership period, for example as a result of corporate name changes or mergers.

4. Practices On Identity Provider Registration

An IdP registering to the federation needs to be manually approved by a team member of the federation operator.

Such approval requires:

- having an affiliation agreement with RedIRIS, which includes the designation of an official representative
- installing compatible Identity Provider software, and performing compliance tests between the IdP and the federation
- implementation of a minimum mandatory set of attributes[3] (and some optional ones, if necessary)
- a completed SIR membership service agreement validated by the official representative of the newly participating institution

Subsequent changes to these elements and attributes require re-approval by the federation operator.

When requesting access to an SP, the federation operator will generate, publish and maintain the appropriate metadata view.

5. Practices on Service Provider Registration

Each SP must be manually approved by the federation operator in order to be registered with the federation.

All SPs must:

- Use any of the supported protocols in SIR2
- Pass the compatibility tests between the SP and the federation
- A completed SIR membership service agreement signed by the official representative of the newly participating service provider

It is the duty of the Federation operator to review and approve all the details provided by the SP administrator. In addition, a Federation operator can reject changes or further modify details of an SP before approving it. After approving the details about a new SP, the user who requested to register it becomes its first SP administrator. An SP administrator can transfer the administration right to further users.

Only users with administrator rights for a specific SP are able to request modification on its elements and attributes. Such changes require re-approval by a Federation operator.

[3] The list of recommended attributes for the SIR2 federation is available at:

http://www.rediris.es/sir2/federacion/atributos/.

5.1 Additional Rules for Outsourced Service Providers

An Outsourced SP typically hosts a service on behalf of an affiliated institution, for example outsourced email on a commercial provider. It does not refer to SPs which own and host the service themselves, being these part of a commercial entity or an affiliated institution.

It is the duty of the Federation operator to review and approve all the details provided by the representative(s) of the affiliated institution. In addition, a Federation operator can reject changes or further modify details of an Outsourced SP before approving it.

5. Practices regarding metadata modifications

In SIR, metadata gets modified by a Federation operator on behalf of any entity.

The source for generating federation metadata are existing metadata files per entity, which are aggregated into a single view. The Federation generates per-entity files under request from the entity. There's also the possibility of generating subgroups of entities containing both service and identity providers.

5. Referencias

[1] http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[2] http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf

[3] http://saml2int.org/

[4] http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-200509.pdf

[5] http://middleware.internet2.edu/dir/

[6] http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200804.pdf

[7] https://svn.middleware.georgetown.edu/cpp-sp/branches/Rel_1_3/schemas/shibboleth-metadata-1.0.xsd

[8] http://papi.rediris.es/rep/PAPI_Protocol_Detailed.pdf

[9] http://openid.net/developers/specs/

[10] Aclarar enlaces tras hablar con PRiSE sobre versiones de CAS soportadas

[11] http://openid.net/specs/openid-connect-core-1_0.html