iAMRES Identity Federation

Metadata Registration Practice Statement

Authors: A. Todosijević

Publication date: 20.10.2021.

Version: 1.0

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 terms are used in this document:

- **Identity Federation or iAMRES Identity Federation** is the AMRES service by which identity federation is realized for AMRES needs, and within which Home organisations and Service Providers cooperate with the aim of authentication and exchange of appropriate data about end users in order to enable use of service.
- **iAMRES Federation Operator** is the organization that provides identity federation services as described by the Terms for provision of identity federation services. Federation operator for iAMRES Identity Federation is AMRES.
- **Identity Federation User** is AMRES user who has signed the agreement for Identity Federation User. Identity Federation User may be in capacity of Home organisation and/or Service Provider.
- **Identity Federation Partner** is a legal entity that does not have the status of AMRES user, and that has signed agreement for Identity Federation Partner. Identity Federation Partner may be exclusively in capacity of Service Provider.
- **Terms for provision of identity federation services** – A document describing the obligations, rights and expectations of the Federation members and the Identity Federation Operator, User and Partner.
- **Registered Representative** – Individuals authorized to act on behlaf of the Federation User or Partner.
- **Entity** – A discrete component that a Federation User or Partner wishes to register and describe in metadata. This is typically an Identity Provider or Service Provider.

Introduction and Applicability

The purpose of this document is to describe metadata registration practices of the iAMRES Identity Federation.

This document is effective immediately starting from the publication date.

Member Eligibility and Ownership

The procedure for becoming a member of the Identity Federation is described in the Terms for provision of identity federation services document.

AMRES will register SAML entities on behalf of Federation Partners and Users.

AMRES may choose to register SAML entities during (i.e., before the completion of) the formal joining process in good faith that the procedure will be finished within a reasonable time. This is to avoid having dependencies between technical and non-technical issues that delay the joining process unduly. After that the entity will either be formally registered or removed.

AMRES may also chouse to sponsor the registration of SAML entities in the exceptional case where a service is considered to be of value to federation members but the party responsible for the SAML entity is not currently willing or able to formally join the Federation at that time.

The Entity eduGAIN publishing policy varies:

- Identity Providers follow an opt-out policy, so they are published to eduGAIN, unless specified differently by the User they belong to.
- Service Providers follow an opt-in policy: they are published to eduGAIN only if the User or the Partner they belong to explicitly ask for the eduGAIN publishing.

To register a new entity, the Registered Representative needs to send request to AMRES via e-mail helpdesk@amres.ac.rs.

Metadata Format

Referenced SAML Metadata Specifications, by XML namespace declaration used:

- `md`: SAML V2.0 Metadata
- `mdattr`: https://wiki.oasis-open.org/security/SAML2MetadataAttr
- `mdrpi`: https://wiki.oasis-open.org/security/SAML2MetadataDRI
- `mdui`: https://wiki.oasis-open.org/security/SAML2MetadataUI
- `shibmd`: https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt

Metadata for all entities registered by the Federation Operator shall make use of the metadata extension to indicate that the iAMRES Federation Operator is the registrar for the entity and to detail the version of the MRPS statement that applies to the entity. The following is a non-normative example:

<mdrpi:RegistrationInfo registrationAuthority="https://federacija.iamres.ac.rs/" registrationInstant="2021-09-22T12:39:00Z">
  <mdrpi:RegistrationPolicy xml:lang="en">https://www.amres.ac.rs/en/institutions/iamres-identity-federation/mrps </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>

Entity Eligibility and Validation

For each entity, AMRES is responsible for verifying that:

- All required information is present in the metadata;
- Metadata is correctly formatted;
- Identity federation User or Partner has the right to use particular domain names in relation to entityID attributes;
- EntityID values are an absolute URI using http, https or urn schemes;
- Only necessary attributes are requested;
- Text content elements properly represents the organization or service(s) concerned;
- URLs specified in the metadata are technically reachable;
- Protocol endpoints are properly protected with TLS/SSL certificates.

Entity Management

Once a Federation User or Partner has joined the iAMRES Identity Federation new entities may be added, modified or removed by the organisation with the approval of the Federation Operator.

To change or remove an entity that has already been registered, the Registered Representative needs to send request to AMRES via e-mail helpdesk@amres.ac.rs.

AMRES may amend or modify the Identity federation metadata at any time in order to, for example, but not limited to:

- ensure the security and integrity of the metadata;
- comply with Interfederation agreements;
- improve interoperability, or
- generally add value to the metadata.