Interfederation Technical Policy

Interfederation Technical Policy Rules

Metadata Import Policy

> **Basic Metadata Import Policy**
>
> Global metadata is imported directly into the main production aggregate.

For the v9 deployment of the metadata aggregator (released 2019-03-20), the following import rules will be implemented (in order):

1. Silently remove all imported entities with XML attribute `mdrpi:RegistrationInfo[@registrationAuthority='https://incommon.org']`
    a. Entities so marked must come from primary sources only.
2. Remove (and log the removal of) the following XML elements (not entities):
    a. `<mdui:Logo>` elements (not entities) with a URL that is not HTTPS-protected
3. Silently remove the following XML elements (not entities):
    a. all MDUI metadata (e.g., `mdui:UIInfo` elements) within `AttributeAuthority` roles.
    b. all entity attributes on the Entity Attribute Blacklist (see subsection below).
    c. all extended XML elements and attributes defined in namespaces not on the XML Namespace Whitelist (see subsection below).
4. Remove (and log the removal of) all imported entities matching one or more of the following conditions:
    a. Entities with an entityID that does not begin with one of the following prefixes: “`http://`”, “`https://`”, “`urn:mace`”
    b. Entities with weak keys (which includes all keys less than 2048-bits in length)
        i. The use of weak keys in metadata has security and privacy implications.
        ii. There are no weak keys in InCommon metadata and so we'd like to keep it that way.
    c. IdP entities with a faulty `<shibmd:Scope>` element
        i. Require regexp attribute on `<shibmd:Scope>`
        ii. Values which do not represent a permissible scope:
            1. `regexp="false"` scope values must:
                a. be syntactically valid domain names (for example, they may not be empty or contain white space), and
                b. must represent domains under a "public suffix" such as `.com` or `.edu` listed in the public suffix list
            2. `regexp="true"` scope values must:
                a. not be empty or include white space, and
                b. must end with:
                    i. an escaped dot ('`\.`'),
                    ii. followed by a "literal tail", which must:
                        1. consist of at least two domain labels (e.g., "`example`", "`edu`") separated by encoded dots ('`\.`'),
                        2. which when the encoded dots are decoded represents a domain name under a "public suffix" such as `.com` or `.edu` listed in the public suffix list
                    iii. followed by a '$' anchor
    d. IdP entities that do not have a SAML2 SingleSignOnService endpoint that supports the HTTP-Redirect binding.
        i. In effect, all imported IdPs must support SAML2.
    e. SP entities that do not have at least one SAML2 AssertionConsumerService endpoint that supports the HTTP-POST binding.
        i. In effect, all imported SPs must support SAML2.
    f. Entities containing literal CR characters.
    g. Entities containing misplaced or duplicated `EntityAttributes` elements.
    h. Entities containing XML failing schema validation.
    i. Entities that do not conform to the SAML v2.0 Metadata Profile for Algorithm Support Version 1.0
    j. Entities that do not follow standard rules regarding Binding values on protocol endpoints in metadata
    k. Entities that do not conform to the SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0
    l. Entities that do not conform to the Identity Provider Discovery Service Protocol and Profile
    m. Entities that do not conform to the Service Provider Request Initiation Protocol and Profile Version 1.0
    n. Entities that do not conform to the SAML V2.0 Metadata Interoperability Profile
    o. Entities that do not conform to the SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0
    p. Entities that do not conform to the SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0
    q. Entities that do not conform to the REFEDS Research and Scholarship Entity Category
    r. Entities that do not conform to the REFEDS SIRTFI specification
    s. Entities that do not conform to the SAML V2.0 Metadata specification
    t. SP entities with an endpoint location that is not HTTPS-protected
    u. Entities that do not conform to the ADFS Metadata Profile
    v. Entities that have inconsistent metadata for SAML 1.x support
    w. Entities that have errors in their `RequestedAttributes` elements
5. Silently remove all imported entities that have the same entityID as an existing entity in the InCommon aggregate.
    a. This happens because some SPs choose to join multiple federations.
    b. Dozens of global SPs are filtered by this rule.

A number of additional rules are applied to ensure metadata correctness. Some common minor errors are corrected but entities failing checks such as XML schema validity are removed.

Log all of the following:

View the published import filter logs

- entities filtered by an import rule
- entities removed for lack of schema validity
- entities modified in any way

Entity Attribute Blacklist

Name	Value
http://macedir.org/entity-category	http://id.incommon.org/category/registered-by-incommon
http://macedir.org/entity-category	http://id.incommon.org/category/research-and-scholarship
http://macedir.org/entity-category-support	http://id.incommon.org/category/research-and-scholarship
urn:oasis:names:tc:SAML:attribute:assurance-certification	http://id.incommon.org/assurance/bronze
urn:oasis:names:tc:SAML:attribute:assurance-certification	http://id.incommon.org/assurance/silver

XML Namespace Whitelist

Namespace	Prefix
urn:oasis:names:tc:SAML:metadata:algsupport	alg
http://www.w3.org/2000/09/xmldsig#	ds
urn:oasis:names:tc:SAML:2.0:profiles:holder-of-key:SSO:browser	hoksso
http://id.incommon.org/metadata	icmd
urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol	idpdisc
urn:oasis:names:tc:SAML:profiles:SSO:request-init	init
urn:oasis:names:tc:SAML:2.0:metadata	md
urn:oasis:names:tc:SAML:metadata:attribute	mdattr
urn:oasis:names:tc:SAML:metadata:rpi	mdrpi
urn:oasis:names:tc:SAML:metadata:ui	mdui
http://refeds.org/metadata	remd
urn:oasis:names:tc:SAML:2.0:assertion	saml
urn:mace:shibboleth:metadata:1.0	shibmd
http://www.w3.org/2001/04/xmlenc#	xenc
http://www.w3.org/XML/1998/namespace	xml
http://www.w3.org/2001/XMLSchema-instance	xsi

Metadata Export Policy

Basic Metadata Export Policy

InCommon Operations refreshes the export aggregate daily, in conjunction with the daily metadata-signing process.

1. **IdPs are exported by default** (but may choose to opt out)
2. **SPs actively opt in** to the export process

InCommon Operations reserves the right to prevent any entity from being exported.

The following export rules have been implemented:

1. Filter all entities **not** having XML attribute `mdrpi:RegistrationInfo[@registrationAuthority='https://incommon.org']`
    a. Only entities registered by InCommon will be exported.
2. Filter the legacy incommon.org R&S entity attribute value from exported SP entity metadata:
    a. `http://id.incommon.org/category/research-and-scholarship`

   b. This legacy attribute value remains in SP metadata for backwards compatibility only. We intend to completely remove this attribute value from SP metadata in the future.
   c. This legacy attribute value has nothing to do with R&S interoperability outside of the InCommon Federation.
3. Filter SAML1-only entities:
   a. An SP entity **not** having at least one SAML2 `AssertionConsumerService` endpoint that supports the HTTP-POST binding will **not** be exported.
   b. An IdP entity **not** having a SAML2 `SingleSignOnService` endpoint that supports the HTTP-Redirect binding will **not** be exported.

Extension schema required for exported metadata

Namespace	Prefix
http://id.incommon.org/metadata	icmd
http://refeds.org/metadata	remd
http://www.w3.org/2000/09/xmldsig#	ds
http://www.w3.org/2001/XMLSchema-instance	xsi
http://www.w3.org/XML/1998/namespace	xml
urn:mace:shibboleth:metadata:1.0	shibmd
urn:oasis:names:tc:SAML:2.0:assertion	saml
urn:oasis:names:tc:SAML:2.0:metadata	md
urn:oasis:names:tc:SAML:metadata:attribute	mdattr
urn:oasis:names:tc:SAML:metadata:rpi	mdrpi
urn:oasis:names:tc:SAML:metadata:ui	mdui
urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol	idpdisc