

Appendix A: Technical requirements

Approved by Kalmar Union steering committee 25.10.2010.

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 RFC2119.

Publishing entities from local federation to Kalmar

A participating federation **MUST** only publish local entities to the Kalmar Metadata Service that are Kalmar-enabled. A Kalmar-enabled entity means that the entity is aware of Kalmar and consuming Kalmar metadata.

A Kalmar-enabled *Identity Provider* will be technically interoperable with all Kalmar Service Providers. It **SHOULD** be technically capable of automatically adopting the attribute release policy stated in the metadata.

A Kalmar-enabled *Service Provider* will be technically interoperable with all Kalmar Identity Providers. It **SHOULD** allow the user to select from all Kalmar Identity Providers.

Even, if Kalmar requires entities to be technically interoperable, there may be business policy reasons to why an entity may only communicate with a subset of other Kalmar entities - this is acceptable.

If a Service Provider (with the same entityID) is registered both to Kalmar and a national federation (other than the one who published it to Kalmar), the Service Provider's entity in the national federation's metadata **SHOULD** prevail.

SAML 2.0 Web Single Sign-On Profile

Entities that participate in the Kalmar Union **MUST** support *SAML 2.0* as specified by OASIS. The Kalmar Union furthermore specifies a deployment profile that specifies how to configure the *SAML 2.0* entities in Kalmar. The Kalmar Union entities **MUST** follow the [Interoperable SAML 2.0 Web Browser SSO Deployment Profile version 0.2](#).

Each participating federation **MUST** ensure that all participating entities have a *SAML 2.0 EntityID* in a controlled namespace, in order to avoid conflicting IDs. For example a university that uses an URL as entityID **MUST** use a domain name that the university or the federation control.

There might be Service Providers that are already part of more than one of the participating federations. A Service Provider **MUST** only be exposed to Kalmar through one federation. A federation **MUST NOT** publish a Service Provider to Kalmar that already is available in Kalmar through another federation.

SAML 2.0 Single Logout

In the Kalmar Union it is OPTIONAL to support global logout. Support to logout is manifested by having a `SingleLogoutService` endpoint present in the entity's SAML 2.0 Metadata document.

If an entity supports single logout it MUST follow the following guidelines:

- Use the HTTP-REDIRECT binding both for the LogoutRequest and for the LogoutResponse
- Processing an incoming logout request MUST respect the `IsPassive` flag, if set in the request.
- The entity MUST ensure that the session is torn down in the application layer as well.

If the entity is not supporting single logout with the limitations mentioned above, it MUST NOT expose its SAML 2.0 logout endpoints in the provided SAML 2.0 Metadata document.

Federations SHOULD make sure that the providers exposing a single logout endpoint in the national aggregate have actually tested the logout functionality against the guidelines above.

Attributes in Kalmar

All attributes transferred in Kalmar MUST use the OID formatting of attribute names. This to ease interoperability across federations and with other inter-federation initiatives. The NameFormat MUST be `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`. This is aligned with the *MACE-Dir Attribute Profile for SAML 2.0*.

Each participating federation have different requirements for which attributes the Identity Provider MUST support. An updated overview is available at:

- <http://www.kalmar2.org/kalmar2web/attributes.html>

The participating federations SHOULD ensure that SPs in the federation aggregate do not request the *National Identification Number* (`schacPersonalUniqueID`) attribute or any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life. Registering a Service Provider requesting aforementioned data is allowed only on Kalmar union steering committee's decision.

All participants (service providers, institutions and federations) MUST support the schema defined in [eduPerson](#). Other schemas supported include SCHAC, funetEduPerson, norEduPerson, eduOrg, norEduOrg and norEduOrgUnit.

Background information about attribute OIDs and names can be found at:

- http://rnd.feide.no/2009/03/20/attribute_names_to_oid_-_machine_readable/

More information about attribute requirements and attribute schemas is available at <http://www.kalmar2.org>.

References:

- [MACE-Dir SAML Attribute Profiles](#)

SAML 2.0 Metadata

Each participating federation MUST provide a metadata aggregate of all entities that should be exposed in the Kalmar Union. These entities are presented in a *SAML 2.0 XML Metadata Document*. This document MUST be made available on a publicly available URL, and it MUST be signed. The URL to the document and the public signing key will be configured in the central Kalmar Union Metadata aggregator.

All entities exposed in the national aggregates MUST be properly configured to consume Kalmar metadata from the central aggregate.

Both the metadata document provided by federations and by the aggregator MUST contain a `EntitiesDescriptor` as the root node with `EntityDescriptor`-s as children, and not contain nested `EntitiesDescriptor`-s.

Name and description of entities

Service Providers in Kalmar MUST be presented with a descriptive name of the service that the Service Provider represents (not the name of the company) in at least English. Service Providers MUST also be given a longer description in at least English, that explains what the service offers. The name and description SHOULD take into consideration a wider audience than the local federation, and be understandable by users in other federations (countries).

The name and description of a Service Provider MUST be using the `AssertionConsumerService/ServiceName` and `AssertionConsumerService/ServiceDescription` elements.

Example of metadata including name and description of a Service Provider in Kalmar:

```
<AttributeConsumingService index="0">
  <ServiceName xml:lang="en">Foodle</ServiceName>
  <ServiceDescription xml:lang="en">Foodle is a generic poll and survey tool for deciding
    meeting dates.</ServiceDescription>
  <ServiceDescription xml:lang="no">Foodle er et generisk poll og survey verkt&#xF8;y for
    &#xE5; bli enige om m&#xF8;tedatoer.</ServiceDescription>
  <ServiceDescription xml:lang="nn">Foodle er eit generisk poll- og survey-verkt&#xF8;y
    for &#xE5; verte einige om m&#xF8;tedatoar.</ServiceDescription>
```

Identity Providers in Kalmar MUST be presented with a descriptive name. If the Identity Provider represents a whole federation, the name SHOULD make it obvious to users if they are represented by this Identity Provider or not. If the Identity Provider represents an institution, the name MUST be set to the full name of

that institution. The name of an Identity Provider **MUST** be represented in metadata using the EntityDescriptor/Organization/OrganizationDisplayName element.

Example of the name of an Identity Provider, representing a whole federation:

```
<Organization>
  <OrganizationName xml:lang="en">Feide - Norwegian Educational and Research
    Institutions</OrganizationName>
  <OrganizationName xml:lang="no">Feide - Norske utdannings og
    forsknings-institusjoner</OrganizationName>
  <OrganizationDisplayName xml:lang="en">Feide - Norwegian Educational and Research
    Institutions</OrganizationDisplayName>
  <OrganizationDisplayName xml:lang="no">Feide - Norske utdannings- og
    forsknings-institusjoner</OrganizationDisplayName>
  <OrganizationURL xml:lang="en">http://www.feide.no/introducing-feide</OrganizationURL>
  <OrganizationURL xml:lang="no">http://www.feide.no/</OrganizationURL>
</Organization>
```

Example of the name of an Identity Provider, representing an institution:

```
<Organization>
  <OrganizationName xml:lang="fi">Turun yliopisto</OrganizationName>
  <OrganizationName xml:lang="en">University of Turku</OrganizationName>
  <OrganizationDisplayName xml:lang="fi">Turun yliopisto</OrganizationDisplayName>
  <OrganizationDisplayName xml:lang="en">University of Turku</OrganizationDisplayName>
  <OrganizationURL xml:lang="fi">http://www.utu.fi</OrganizationURL>
  <OrganizationURL xml:lang="en">http://www.utu.fi</OrganizationURL>
</Organization>
```

The use of acronyms in name and description is discouraged. It is RECCOMENDED to offer name and descriptions in all of the native languages of the participating federations.

Metadata validity period

Kalmar entities **MUST** always be associated with a limited validity time period, by the use of the validUntil attribute in the metadata document. This attribute may be set on either the root node (EntitiesDescriptor) or the entity node itself (EntityDescriptor).

Entities published through federation aggregate MUST (at the time fetched) have a validity period longer than 6 hours, and less than 240 hours. If the `cacheDuration` attribute is set, it MUST be longer than 6 hours.

Federations are encouraged to use validity windows of at least 72 hours, which will allow a repair-time through a weekend. (In example: Problem occur on Friday afternoon, and fixed during Monday).

The Kalmar aggregator will fetch and cache metadata from all sources at least once an hour. Entities when re-distributed by the aggregator will adopt the validity period from the source, and calculate a new expiration time based up-on the `validUntil` values (may be one or two) and the `cacheDuration` values. The resulting validity period will be upper limited to 96 hours.

Consequently metadata consumed from the Kalmar aggregator will at the time fetched have a validity period between 5 and 96 hours.

Attribute Release Policy

Kalmar Service Providers MUST express its needed set of attribute through metadata. The participating federation is responsible for accepting and moderating the requested attributes for all of its entities. Strict policy MUST be enforced for the list of requested attributes, as Identity Providers will release these attributes without further moderation or consideration.

```
<AttributeConsumingService index="0">
  <ServiceName xml:lang="en">Example Service Provider</ServiceName>
  <ServiceDescription xml:lang="en">Description of the SP.</ServiceDescription>
  <RequestedAttribute
    Name="urn:oid:1.3.6.1.4.1.25178.1.2.9"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
  <RequestedAttribute
    Name="urn:oid:2.5.4.10"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
  <RequestedAttribute
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.5"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
</AttributeConsumingService>
```

The Kalmar aggregator also provides a separate document summarizing attribute release policy of all Kalmar entities in a Shibboleth specific Attribute Release Policy XML document.

Extensions

The aggregator is aware of the following Metadata Extensions:

urn:mace:shibboleth:metadata:1.0

urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol

The Kalmar aggregator drops the entities with Metadata Extensions that it is not aware of.

Scopes

All Identity Providers entities **MUST** include a list of *scopes*. Scopes restricts the realms that the IdP is authorized to assert scoped attributes under. In example, if an Identity Provider includes scopes for `uio.no` and `uit.no`, and the Identity Provider tries to issue an `eduPersonPrincipalName` (a scoped attribute) with the value of `john.doe@uib.no`, then the Service Provider **SHOULD** reject this attribute.

The use of the `Scope` element in metadata is specified in the [Shibboleth Metadata Profile](#). In Kalmar the `regexp` attribute **MUST** be set to `false`. The `Scope` element(s) **MUST** be placed in the `EntityDescriptor/IDPSSODescriptor/Extensions` container.

```
<EntityDescriptor entityID="https://tullbommen.arcada.fi/simplesaml/">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
        regexp="false">arcada.fi</shibmd:Scope>
    </Extensions>
  </IDPSSODescriptor>
</EntityDescriptor>
```

Monitoring

Each participating federation is advised to setup monitoring and alerts for its own metadata export, to be able to discover and repair errors within the validity period of the metadata.

User consent

Consent management at the IdP is handled within each federation.

Identity Provider discovery

Services connected to the Kalmar Union are responsible for the user interface for selecting which IdP to login to. [The Identity Provider Discovery Service Protocol and Profile](#) is RECOMMENDED by Kalmar.

Kalmar offers a central discovery service supporting this profile. Using the central discovery service is **OPTIONAL**. Services may use the central discovery service, either as stand alone or for complementing other discovery services.

Signing and encryption keys

All IdP entities MUST have an embedded signing certificate in the metadata. All SP entities MUST have an embedded certificate for encryption use if its endpoints are not available on HTTPS.

The use of embedded keys in metadata MUST follow the guidelines of this document:

[SAML V2.0 Metadata Interoperability Profile \(DRAFT\)](#)

Identity Management

Information about requirements for identity management procedures for any Kalmar2-enabled user account are provided by each participating federation, and MUST be available in English. All users MUST go through documented procedures for proofing of identity, authentication methods, quality and freshness of attributes released about the user from the identity provider.

Information about users SHOULD be updated every working day. Accounts SHOULD be closed within two weeks after the user's grace period for belonging to the home organization. Identity proofing MUST happen in accordance with national best practice. Authentication methods SHOULD be according to national levels of assurance definitions.

Currently there is only one level of assurance for identity, authentication or attributes.

Persistent identifier

As an end user's persistent identifier, either `eduPersonTargetedID/PersistentID` or `eduPersonPrincipalName` MUST be available in the IdPs. Kalmar union encourages the use of `eduPersonTargetedID/PersistentID` for enhanced privacy.

Both SAML2 Persistent ID in the SAML assertion's Subject NameID element and `eduPersonTargetedID` in an attribute statement can be used in Kalmar. To ensure user consent to release of personal data,

an IdP releasing persistentID in Subject NameID MUST release `eduPersonTargetedID` as an attribute statement, as well.

an IdP releasing `eduPersonTargetedID` as an attribute statement must release persistentID in Subject NameID, as well.

in both cases, the IdP MUST provide the same value for both the persistent ID and the `eduPersonTargetedID` attribute.

Privacy policy

Privacy policy information is provided by each participating federation.

Haka privacy policy engine (<https://haka.funet.fi/cgi-bin/privacypolicy>) where each of Haka's SPs has registered the URL of its privacy policy. Haka uses the privacy policy engine to inform end users about release of their personal data.

Feide requires each Service Provider to provide privacy policy.

WAYF has no requirements to the service providers as this is covered by existing legislation.

Contacts for administrative and technical issues

The participating federations' contacts for administrative and technical issues are published in the Kalmar Union web site.