

Appendix A: Technical requirements

Version 1.0

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.

Federation architecture

The Kalmar2 environment consists of a full mesh of all the IdPs and SPs that each participating federation share in the Kalmar2 union. All participating Service Providers are visible to the Identity Providers.

WebSSO 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 (<http://saml2int.org>).

Each participating federation (country) MUST ensure that all participating entities have an 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.

Single Logout Profile

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.

National 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.

Metadata management

Each participating federation (country) MUST provide a national 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 signing public key will be configured in the central Kalmar Union Metadata Aggregate.

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

On each entity in the national metadata there MUST be set a value for expiration of the metadata using the validUntil attribute. The validUntil value MUST be set to a timestamp between 6 hours and 96 hours.

All Identity Providers entities MUST include a list of 'scopes'. Scopes restricts the realms that the IdP is authorized to assert so called 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 syntax of the scope-list in metadata follows the Shibboleth shibmd:Scope syntax.

All Service Provider entities MUST include a list of requested attributes. A separate document describes what information MUST be present in metadata for entities in Kalmar. This document goes through metadata for both SP and IdP by using examples:

- Kalmar metadata by example (<https://rnd.feide.no/content/kalmar-metadata>)

Although the official and authoritative information about attribute release policy is included in the metadata itself, using RequestedAttribute, Kalmar supports providing Shibboleth specific Attribute Release Policy XML documents in order to make it convenient for new Identity Providers using Shibboleth to automatically adopt a attribute release policy that matches the Kalmar metadata. Background information about Kalmar ARPs (<https://kalmar.feide.no/simplesaml/arp/kalmar-haka-arp.xml>) and the Haka federation Shibboleth1.3 ARP (<https://haka.funet.fi/fed/arp.site.xml>).

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 (<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf>) is RECOMMENDED by Kalmar.

Kalmar offers a central 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 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) (<https://spaces.internet2.edu/download/attachments/11275/draft-sstc-metadata-iop-01.pdf?version=2>)

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 PersistentID 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 SP requesting persistentID in Subject NameID MUST request eduPersonTargetedID as an attribute statement, as well.

To ensure that an SP can pick up any of the two, an IdP releasing both the persistentID and the eduPersonTargetedID attribute MUST provide the same value for them.

Other attributes

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'.

Each participating federation have different requirements for attributes. An updated overview is available at: <http://www.kalmar2.org/kalmar2web/attributes.html>

The national federations SHOULD ensure that SPs in the national 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 as a minimum support the schema defined in 'eduPerson' (<http://middleware.internet2.edu/eduperson/>). Other schemas supported include SCHAC, funetEduPerson, norEduPerson, eduOrg, norEduOrg and norEduOrgUnit.

Background information about attribute OIDs and names can be found at <https://rnd.feide.no/content/attribute-names-oid-machine-readable> .

Information about attribute requirements is available at <http://www.kalmar2.org> .

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.