Appendix 1
Technical Requirements

Version 2.4.7

Technical requirements for membership in the Skolfederation

The Skolfederation has, like many other federation initiatives, the goal to use the following SAML[1]-profiles:

- eGov[2] 2.0
- saml2int[3], the Interoperable SAML 2.0 Profile

This appendix shows a selection of the most important SAML capabilities from the eGov2 implementation profile and the requirements that saml2int poses on them.

Requirements on Members

Service Provider, SP

A Service Provider is a Party that supplies a service that Users gain access to, based on an Assertion from an Identity Provider. The Service Provider often states requirements on Identification concepts, required Attributes and Level of Assurance, LoA.

1 Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language 2.0 (SAML)

2 Kantara Initiative eGov 2.0 profile

3 Interoperable SAML 2.0 Web Browser SSO Deployment Profile, http://saml2int.org/

Identity Provider, IdP

An Identity Provider is an organization, or equivalent, that supplies a User with a digital Identity and Attributes. The Identity Provider also issues Assertions based upon these within the Skolfederation. It is presupposed that the Identity Provider has access to the registers needed to be able to supply the Attributes that are requested by the Service Provider.

Federation Operator

One of the most important responsibilities of the Federation Operator is to supply an aggregation of digitally signed SAML metadata. This can be regarded as the technical core of the Federation, which ties the parties in the federation together. The Federation Operator is responsible for the correctness of annotations and extensions of metadata, and that these, if they affect the behavior of Identity Providers or Service Providers, comply with the Federation framework and applicable law.

General Technical Requirements

Key Management

Security requirements for keys for signing and encryption

All Members in the Federation **must** create, manage and store signing and encryption keys in accordance with the requirements that are posed in the Trust Framework of the Skolfederation.

If nothing else is stated, algorithms and key lengths for authentication, encryption and signing **must** follow NIST SP 800-131[4] or ETSI TS 102 176-1[5]. Regarding the choice of algorithm, the requirements can be fulfilled by using SHA-256 and RSA with a key length (modulus) of at least 2048 bits.

Please note that the requirements on key lengths and algorithms are subject to constant evaluation and that the requirements can be changed over time.

The publishing of the Federation Operator´s public key

The Federation Operator´s public key is used for verifying signatures of published metadata. The current key is published in a certificate named skolfederation-VERSION.crt (where VERSION is changed for the version number of the relevant metadata) on the web site of the Skolfederation, www.skolfederation.se.

4 http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

5 http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.01.01_60/ts_10217601v020101p.pdf

Verification of the Federation Operator´s public key

When updating the Federation Operator´s public key in a Member´s local configuration, the Member **must** verify its authenticity against at least two different sources. The following are acceptable verification sources:

- fetch the certificate including the public key directly from **https://www.skolfederation.se,** including a positive verification of the HTTPS certificate that identifies the site of publication (according to Web PKI)
- contact with the Skolfederation support service, where the certificate´s digital SHA-1 fingerprint is verified over telephone.

Change of the Federation Operator´s public key

At planned changes of the Federation Operator´s public key, all Members of the Federation are notified at least 30 days prior to the use of the new key for verification of the signature enclosing published SAML metadata. In order to reduce the risk of using the wrong key, the new key and its associated metadata are published on a web site that differs from earlier keys and metadata by a version change of the URL, as stated above.

Routines for changing a Member´s encryption keys

When changing a Member´s encryption keys, the following steps **should** be performed:

1. The Member conveys SAML metadata including a new certificate, with the new public encryption key, to the Federation Operator for publishing.
2. Until the new encryption key has reached all other parties within the Federation, the Member **should** use double private keys for decryption.

If these steps are not followed, there is a risk for an interruption in the Service until all other parties within the Federation have fetched and started to use the new metadata.

Routines for changing a Member´s signing keys

When changing a Member´s signing keys, the following steps **should** be performed:

1. The Member conveys SAML metadata including both the new and the old certificate with the public signing keys to the Federation Operator for publishing.
2. During a transition period, all other parties **must** use double keys for verifying the authenticity of the signature.
3. When the new key has reached all other parties in the Federation, the Member **should** convey updated SAML metadata, including only the new certificate with the new public signing key to the Federation Operator.

If these steps are not followed, there is a risk for an interruption in the Service until all other parties within the Federation have fetched and started to use the new metadata.

SAML metadata (MD)

In order to enable trust for assertions from other Parties between Members in the Federation, exchange of public keys between the Parties is needed. This exchange is performed through the SAML metadata (MD). The metadata describes the Member´s characteristics, capacities and public keys and are aggregated by the Federation Operator. The Federation Operator performs an analysis of the metadata, prior to signing and publishing the aggregated SAML metadata. The aggregated and signed SAML metadata published by the Federation Operator is hence the collective description of all the Federation actors' characteristics, capacities and public keys.

Publishing of SAML metadata

The address of the Federation´s aggregated and signed SAML metadata is published on the Skolfederation web site, www.skolfederation.se.

Verification of the signed SAML metadata

Every Member **must** verify the digital signature that encloses the SAML metadata at every update of the local copy, using the public key published by the Federation Operator.

SAML metadata format

Saml2int describes how SAML metadata **shall** be presented. The format of SAML metadata is regulated in OASIS *SAML V2.0 metadata specification* [SAML2Meta[6]] and the handling of SAML metadata is regulated in OASIS *Metadata Interoperability Profile* [MetaIOP[7]]. All Members in the Federation **must** support these profiles.

Updating the Skolfederation metadata

The Skolfederation metadata contains a description of how long it may be used, by the attributes *cacheDuration* and *validUntil* of the element EntitiesDescriptor (which is normally the first element in the SAML metadata). The Member **should** normally update his local copy of the Federation Metadata at least with the periodicity that is stated in *cacheDuration.* Depending on the choice of software, this can be done automatically. Metadata **must not** be considered valid after *validUntil.*

Directory Service (DS)

6 http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

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

When a User wishes to use a Service Provider, for which the User is not yet identified, he is asked to identify himself. In a two party relation it is unambiguous which Identity Provider to use for this. In a Federation, such as the Skolfederation, with the possibility for a large number of Identity Providers, a generic function is needed to assign the User to "his" Identity Provider.

A Directory Service uses SAML metadata to show the User the Identity Providers in the Federation.

The address of the central Directory Service in the Federation is published on the Skolfederation web site, www.skolfederation.se.

A central Directory Service is not needed for cooperation within a Federation. The Service Provider can choose to implement his own function for local assigning based on SAML metadata.

Another possibility is to use an *unsolicited response,* which means that the User first connects to his Identity Provider with a parameter in the call, which then is used to assign the User to the correct Service.

The assigning of Identity Providers is regulated in the OASIS *Identity Provider Discovery Service Protocol Profile* [IdPDisco[8]]. All Members of the Federation **should** support this profile.

Pseudonymised Identities (NameID)

A cornerstone for the Skolfederation is to continuously protect personal integrity. Hence pseudonyms **should** be used as far as possible as the identification concept (NameID).

There are two kinds of pseudonyms. *Persistent pseudonyms,* (permanent), have the characteristic that they always represent the same User in the Service in question. *Transient pseudonyms* (non-permanent) are temporary and are never reused.

When using persistent pseudonyms different pseudonyms are presented for every Service. When using transient pseudonyms a new pseudonym is presented for every occasion and every Service.

Pseudonyms are part of the standard specification for SAML 2.0 [SAML2Core[9]] and the following **shall** be supported:

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient

8 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf

9 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

Authentication Request

When a User wants to access a Service Provider, but has not been identified earlier, he will be asked to identify himself. The Service will create a request called AuthenticationRequest. The User will send this to his Identity Provider through an http-redirect.

Saml2int states how *SAML V2.0 Web Browser SSO Profile* [SAML2Prof[10]] shall be used, including Authentication Requests. The profile states among other things that:

- Communication **should** be protected by TLS/SSL in the transport layer, according to RFC 7525.
- An Identity Provider **may** omit to verify signed Authentication Requests if it can be suspected that they might be used for Denial of Service (DoS) attacks.

Authentication Response

An Authentication Response can be the result of an Authentication Request, but it can also be a response without a prior request. The latter response is called an *unsolicited response*.

Saml2int states how *SAML V2.0 Web Browser SSO Profile* [SAML2Prof] shall be used, including Authentication Responses. The profile states among other things that:

- Communication **should** be protected be TLS/SSL in the transport layer, according to RFC 7525**Fel! Bokmärket är inte definierat.**.
- If TLS/SSL cannot be used, the Authentication Response, *AthenticationResponse,* **should** be encrypted in its entirety with the Service´s public key that is published in the SAML metadata.
- The Authentication Response **shall** be signed with the Identity Provider´s private key, where the corresponding public key is published in the SAML metadata.
- Service Providers **must** accept *unsolicited responses.*
- Service Providers **must** verify signatures with the Identity Providers´ public key that is published in the SAML metadata.
- Service Providers **shall** decrypt responses with the private key corresponding to the Service´s public key that is published in the SAML metadata.
- The Service and the Identity Provider **shall** be able to manage multiple keys, in order to enable the exchange of keys.
- Certificates in the SAML metadata **shall** only be considered as bearers of the public key. No method for the verification of the certificates´ validity may be used. All keys found in the SAML metadata **shall** be considered as valid.
- Keys that are not in use **must** be removed from the SAML metadata.

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

Managing different Levels of Assurance (LoA)

The Skolfederation has the intention to be able to manage different Levels of Assurance. It is the Service Provider that chooses the Level of Assurance needed based on how sensitive its information is. Members must be able to exchange information regarding which Levels of Assurance Identity Providers can offer and which level Service Providers request. The information regarding Levels of Assurance can be added to the SAML metadata, as well as within an Authentication Request and an Authentication Response.

Information regarding the Level of Assurance in the SAML metadata has the advantage that a Directory Service can reduce the selection of Identity Providers for a User. Only those that fulfil the requested Level of Assurance need to be shown.

In the SAML metadata, the Level of Assurance is represented by one or more Attribute. All Members **should** be able to manage extended SAML metadata that allows the presentation of Attributes according to *SAML V2.0 Metadata Extension for Entity Attributes*[11]. The Attributes for Level of Assurance are shown according to *SAML V2.0 Identity Assurance Profiles 1.0*[12] and have the following names:

- http://id.skolfederation.se/loa/bas
- http://id.skolfederation.se/loa/2fa
- http://id.skolfederation.se/loa/loa2
- http://id.skolfederation.se/loa/loa3

Levels of Assurance in Authentication Requests and Responses

Exchange of information regarding Level of Assurance concerning an Authentication Request and an Authentication Response give the possibility to manage the fact that an Identity Provider can represent different categories of Users, where it is not evident that the Users´ identities have the same Level of Assurance. Furthermore, a User can have access to different methods for authentication, which lead to different Levels of Assurance. Exchange of such information is performed according to *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*[13]. All Levels of Assurance are presented as an Authentication Context. This presentation of the Levels of Assurance is performed according to *SAML V2.0 Identity Assurance Profiles*.

The Levels of Assurance for the Skolfederation are referenced by a specific URI for every level. They define the authentication classes:

11 http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf

12 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf

13 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

- http://id.skolfederation.se/loa/bas
- http://id.skolfederation.se/loa/2fa
- http://id.skolfederation.se/loa/loa2
- http://id.skolfederation.se/loa/loa3

This URI is found in the schema as targetNamespace.

The Attribute governingAgreementRef in the element GoverningAgreement in the schema contains a URL that refers to the external documentation that defines the level.

The signaling of Levels of Assurance in Authentication Requests and Responses **shall** be handled within AuthnContextClassRef.

In an Authentication Request where a Level of Assurance is requested, the Attribute [Comparison] **must** be set to “exact” or be left out. Certain SAML software products support only exact matching of <saml:AuthnContextClassRef>. If [Comparison] is left out, it **must** be interpreted as “exact”, according to SAML-Core-2.0.

To eliminate problems for a User that already is authenticated with a higher Level of Assurance, an Authentication Request **should** contain all Levels of Assurance that fulfil the Service´s requirements. A set of Levels of Assurance **shall** be interpreted as an ordered list, where the first element represents the preferred level.

If no Level of Assurance is requested, all signaled levels shall be accepted as well as the absence of signaling of level. In practice this means that only the lowest Level of Assurance in the federation can be assured, which is equivalent to [http://id.skolfederation.se/loa/bas]. The “Bas” level implies no other requirements than membership in the Skolfederation.

It is always the consumer of the Authentication Response that has the responsibility to make a correct judgement of the Level of Assurance in the response. If the response is incorrect and lacks the signaling of Level of Assurance, no level can be presupposed.

A schema for the context classes is found in http://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml and also later in this document.

Lack of support for managing Levels of Assurance

All Members **should** support exchange of information on Levels of Assurance in SAML metadata and in Authentication Requests and Authentication Responses.

A Member that does not support the management of different Levels of Assurance shall be considered to belong to the Level of Assurance http://id.skolfederation.se/loa/bas.

Context Class

LoA Bas

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://id.skolfederation.se/loa/bas"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://id.skolfederation.se/loa/bas"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://id.skolfederation.se/loa/bas Defines the
basic level of the Skolfederation.se Assurance Framework
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef"
          type="xs:anyURI"
          fixed="http://id.skolfederation.se/loa/bas"
          use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

LoA 2fa

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://id.skolfederation.se/loa/2fa"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://id.skolfederation.se/loa/2fa"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://id.skolfederation.se/loa/2fa Defines the
strong authentication level of the Skolfederation.se Assurance Framework
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef"
          type="xs:anyURI"
          fixed="http://id.skolfederation.se/loa/2fa"
          use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

LoA 2 (presently not in use)

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://id.skolfederation.se/loa/loa2"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://id.skolfederation.se/loa/loa2"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://id.skolfederation.se/loa/loa2 Defines
Level 2 of the Skolfederation.se Assurance Framework
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef"
          type="xs:anyURI"
          fixed="http://id.skolfederation.se/loa/loa2"
          use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

LoA 3 (presently not in use)

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://id.skolfederation.se/loa/loa3"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://id.skolfederation.se/loa/loa3"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://id.skolfederation.se/loa/loa3 Defines
Level 3 of the Skolfederation.se Assurance Framework
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef"
          type="xs:anyURI"
          fixed="http://id.skolfederation.se/loa/loa3"
          use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

Single Logout (SLO)

The Skolfederation does not, at the moment, require that Members shall support *single-logout*. The Federation does not however restrict Members from implementing *single-logout.*

The technical specification for managing *single-logout* is found in *Single-logout Profile*[14]. It should be noted that session handling is not part of the SAML framework, which makes the matter larger than only a part of a technical specification.

If a Service implements *single-logout* it is important that it is clear from the user interface that a single-logout is carried through, and that the User is logged out from all Services that he is logged in to.

Attribute Authority (AA)

The Skolfederation relies on decentralized provisioning of Attributes where Attributes are provided by Identity Providers, in the same manner as most other federations. A federation can also contain centralized Attribute providers, called Attribute Authorities. The Federation Operator does not at present offer such a central Attribute Authority. There is however no infrastructural restriction that prevents the establishment of such shared Attribute Authorities within the Skolfederation.

Time

It is crucial for the Skolfederation that all Members use a reliable time source. The time source must be traceable to the Swedish national timescale UTC(SP)[15]. This should be implemented using the standardized Network Time Protocol (NTP). The accuracy should never be less than one second.

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

15 http://www.sp.se/sv/index/services/time_sync/ntp/