Authentication Context Classes for Levels of Assurance for the Swedish eID Framework

ELN-0605-v1.1  
Version 1.1

2014-04-28

1 Introduction 3

2 Defined Authentication Context Classes 3

2.1 Level of Assurance – Level 1 3

2.2 Level of Assurance – Level 2 4

2.3 Level of Assurance – Level 3 6

2.4 Level of Assurance – Level 4 7

3 Common XML Schemas 9

3.1 Authentication context parameters 9

4 References 10

5 Changes between versions 10

# Introduction

This specification complements [Eid2Tillit] with definitions of Authentication Context Classes for defined levels of assurance for the Swedish eID framework. These Authentication Context Classes are defined in accordance with Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 [[SAML2AuthCont](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf)].

Each Authentication Context Class defined in this document includes:

* A URI Identifier, which identifies the Authentication Context Class as well as the XML Schema name space for corresponding Authentication Context Declarations.
* The XML Schema for Authentication Context Declarations related to this Authentication Context Class.

# Defined Authentication Context Classes

## Level of Assurance – Level 1

**URI identifier**: http://id.elegnamnden.se/loa/1.0/loa1

**XML Schema**:

<xs:schema targetNamespace="http://id.elegnamnden.se/loa/1.0/loa1"  
 xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://id.elegnamnden.se/loa/1.0/loa1"  
 finalDefault="extension" blockDefault="substitution" version="2.0"  
 xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <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: id.elegnamnden.se/loa/1.0/loa1 defines level 1 of the Swedish E-Identification

board Assurance Framework</xs:documentation>  
 </xs:annotation>  
 <xs:complexType name="AuthnContextDeclarationBaseType">  
 <xs:complexContent>  
 <xs:restriction base="AuthnContextDeclarationBaseType">  
 <xs:sequence>  
 <xs:element ref="GoverningAgreements"/>  
 <xs:element ref="Extension" maxOccurs="1" minOccurs="0"/>  
 </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://elegnamnden.se/doc/tillitsramverk.pdf#loa1" use="required"/>  
 </xs:restriction>  
 </xs:complexContent>  
 </xs:complexType>  
 <xs:complexType name="ExtensionType">  
 <xs:complexContent>  
 <xs:restriction base="ExtensionType">  
 <xs:sequence minOccurs="1">  
 <xs:element ref="loacp:AuthContextParams"/>  
 <xs:element ref="loacp:Other" minOccurs="0"/>  
 </xs:sequence>  
 </xs:restriction>  
 </xs:complexContent>  
 </xs:complexType>  
 </xs:redefine>  
 <xs:import namespace="http://id.elegnamnden.se/ns/1.0/loa-context-params"  
 schemaLocation="loa-context-params.xsd"/>  
</xs:schema>

**Implementation examples**:

The following examples illustrates compliant use of the level 1 XML Schema:

<loa1:AuthenticationContextDeclaration xmlns:loa1="http://id.elegnamnden.se/loa/1.0/loa1">  
 <loa1:GoverningAgreements>  
 <loa1:GoverningAgreementRef governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa1"/>  
 </loa1:GoverningAgreements>  
</loa1:AuthenticationContextDeclaration>

Including authentication context parameters:

<loa1:AuthenticationContextDeclaration xmlns:loa1="http://id.elegnamnden.se/loa/1.0/loa1">  
 <loa1:GoverningAgreements>  
 <loa1:GoverningAgreementRef governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa1"/>  
 </loa1:GoverningAgreements>  
 <loa1:Extension>  
 <loacp:AuthContextParams xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <loacp:AuthContextParam Name="securitycontext"  
 ContentType="base64">EfcC5iQq…</loa:AuthContextParam>  
 <loacp:AuthContextParam Name="othercontext">OtherStuff</loa:AuthContextParam>  
 </loa:AuthContextParams>  
 </loa1:Extension>  
</loa1:AuthenticationContextDeclaration>

## Level of Assurance – Level 2

**URI identifier**: http://id.elegnamnden.se/loa/1.0/loa2

**XML Schema**:

<xs:schema targetNamespace="http://id.elegnamnden.se/loa/1.0/loa2"  
 xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://id.elegnamnden.se/loa/1.0/loa2"  
 finalDefault="extension" blockDefault="substitution" version="2.0"  
 xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <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: id.elegnamnden.se/loa/1.0/loa2 defines level 2 of the Swedish E-Identification

board Assurance Framework</xs:documentation>  
 </xs:annotation>  
 <xs:complexType name="AuthnContextDeclarationBaseType">  
 <xs:complexContent>  
 <xs:restriction base="AuthnContextDeclarationBaseType">  
 <xs:sequence>  
 <xs:element ref="GoverningAgreements"/>  
 <xs:element ref="Extension" maxOccurs="1" minOccurs="0"/>  
 </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://elegnamnden.se/doc/tillitsramverk.pdf#loa2" use="required"/>  
 </xs:restriction>  
 </xs:complexContent>  
 </xs:complexType>  
 <xs:complexType name="ExtensionType">  
 <xs:complexContent>  
 <xs:restriction base="ExtensionType">  
 <xs:sequence minOccurs="1">  
 <xs:element ref="loacp:AuthContextParams"/>  
 <xs:element ref="loacp:Other" minOccurs="0"/>  
 </xs:sequence>  
 </xs:restriction>  
 </xs:complexContent>  
 </xs:complexType>  
 </xs:redefine>  
 <xs:import namespace="http://id.elegnamnden.se/ns/1.0/loa-context-params"  
 schemaLocation="loa-context-params.xsd"/>  
</xs:schema>

**Implementation examples**:

The following examples illustrates compliant use of the level 2 XML Schema:

<loa2:AuthenticationContextDeclaration xmlns:loa1="http://id.elegnamnden.se/loa/1.0/loa2">  
 <loa2:GoverningAgreements>  
 <loa2:GoverningAgreementRef governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa2"/>  
 </loa2:GoverningAgreements>  
</loa2:AuthenticationContextDeclaration>

Including authentication context parameters:

<loa2:AuthenticationContextDeclaration xmlns:loa1="http://id.elegnamnden.se/loa/1.0/loa2">  
 <loa2:GoverningAgreements>  
 <loa2:GoverningAgreementRef governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa2"/>  
 </loa2:GoverningAgreements>  
 <loa2:Extension>  
 <loacp:AuthContextParams xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <loacp:AuthContextParam Name="securitycontext"  
 ContentType="base64">EfcC5iQq…</loa:AuthContextParam>  
 <loacp:AuthContextParam Name="othercontext">OtherStuff</loa:AuthContextParam>  
 </loacp:AuthContextParams>  
 </loa2:Extension>  
</loa2:AuthenticationContextDeclaration>

## Level of Assurance – Level 3

**URI identifier**: http://id.elegnamnden.se/loa/1.0/loa3

**XML Schema**:

<xs:schema targetNamespace="http://id.elegnamnden.se/loa/1.0/loa3"  
 xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://id.elegnamnden.se/loa/1.0/loa3"  
 finalDefault="extension" blockDefault="substitution" version="2.0"  
 xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <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: id.elegnamnden.se/loa/1.0/loa3 defines level 3 of the Swedish E-Identification

board Assurance Framework</xs:documentation>  
 </xs:annotation>  
 <xs:complexType name="AuthnContextDeclarationBaseType">  
 <xs:complexContent>  
 <xs:restriction base="AuthnContextDeclarationBaseType">  
 <xs:sequence>  
 <xs:element ref="GoverningAgreements"/>  
 <xs:element ref="Extension" maxOccurs="1" minOccurs="0"/>  
 </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://elegnamnden.se/doc/tillitsramverk.pdf#loa3" use="required"/>  
 </xs:restriction>  
 </xs:complexContent>  
 </xs:complexType>  
 <xs:complexType name="ExtensionType">  
 <xs:complexContent>  
 <xs:restriction base="ExtensionType">  
 <xs:sequence minOccurs="1">  
 <xs:element ref="loacp:AuthContextParams"/>  
 <xs:element ref="loacp:Other" minOccurs="0"/>  
 </xs:sequence>  
 </xs:restriction>  
 </xs:complexContent>  
 </xs:complexType>  
 </xs:redefine>  
 <xs:import namespace="http://id.elegnamnden.se/ns/1.0/loa-context-params"  
 schemaLocation="loa-context-params.xsd"/>  
</xs:schema>

**Implementation examples**:

The following examples illustrates compliant use of the level 3 XML Schema:

<loa3:AuthenticationContextDeclaration xmlns:loa1="http://id.elegnamnden.se/loa/1.0/loa3">  
 <loa3:GoverningAgreements>  
 <loa3:GoverningAgreementRef governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa3"/>  
 </loa3:GoverningAgreements>  
</loa3:AuthenticationContextDeclaration>

Including authentication context parameters:

<loa3:AuthenticationContextDeclaration xmlns:loa1="http://id.elegnamnden.se/loa/1.0/loa3">  
 <loa3:GoverningAgreements>  
 <loa3:GoverningAgreementRef governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa3"/>  
 </loa3:GoverningAgreements>  
 <loa3:Extension>  
 <loacp:AuthContextParams xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <loacp:AuthContextParam Name="securitycontext"   
 ContentType="base64">EfcC5iQq…</loa:AuthContextParam>  
 <loacp:AuthContextParam Name="othercontext">OtherStuff</loa:AuthContextParam>  
 </loacp:AuthContextParams>  
 </loa3:Extension>  
</loa3:AuthenticationContextDeclaration>

## Level of Assurance – Level 4

**URI identifier**: http://id.elegnamnden.se/loa/1.0/loa4

**XML Schema**:

<xs:schema targetNamespace="http://id.elegnamnden.se/loa/1.0/loa4"  
 xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://id.elegnamnden.se/loa/1.0/loa4"  
 finalDefault="extension" blockDefault="substitution" version="2.0"  
 xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <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: id.elegnamnden.se/loa/1.0/loa4 defines level 4 of the Swedish E-Identification

board Assurance Framework</xs:documentation>  
 </xs:annotation>  
 <xs:complexType name="AuthnContextDeclarationBaseType">  
 <xs:complexContent>  
 <xs:restriction base="AuthnContextDeclarationBaseType">  
 <xs:sequence>  
 <xs:element ref="GoverningAgreements"/>  
 <xs:element ref="Extension" maxOccurs="1" minOccurs="0"/>  
 </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://elegnamnden.se/doc/tillitsramverk.pdf#loa4" use="required"/>  
 </xs:restriction>  
 </xs:complexContent>  
 </xs:complexType>  
 <xs:complexType name="ExtensionType">  
 <xs:complexContent>  
 <xs:restriction base="ExtensionType">  
 <xs:sequence minOccurs="1">  
 <xs:element ref="loacp:AuthContextParams"/>  
 <xs:element ref="loacp:Other" minOccurs="0"/>  
 </xs:sequence>  
 </xs:restriction>  
 </xs:complexContent>  
 </xs:complexType>  
 </xs:redefine>  
 <xs:import namespace="http://id.elegnamnden.se/ns/1.0/loa-context-params"  
 schemaLocation="loa-context-params.xsd"/>  
</xs:schema>

**Implementation examples**:

The following examples illustrates compliant use of the level 4 XML Schema:

<loa4:AuthenticationContextDeclaration xmlns:loa1="http://id.elegnamnden.se/loa/1.0/loa4">  
 <loa4:GoverningAgreements>  
 <loa4:GoverningAgreementRef governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa4"/>  
 </loa4:GoverningAgreements>  
</loa4:AuthenticationContextDeclaration>

Including authentication context parameters:

<loa4:AuthenticationContextDeclaration xmlns:loa1="http://id.elegnamnden.se/loa/1.0/loa4">  
 <loa4:GoverningAgreements>  
 <loa4:GoverningAgreementRef governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa4"/>  
 </loa4:GoverningAgreements>  
 <loa4:Extension>  
 <loacp:AuthContextParams xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <loacp:AuthContextParam Name="securitycontext"   
 ContentType="base64">EfcC5iQq…</loa:AuthContextParam>  
 <loacp:AuthContextParam Name="othercontext">OtherStuff</loa:AuthContextParam>  
 </loacp:AuthContextParams>  
 </loa4:Extension>  
</loa4:AuthenticationContextDeclaration>

# Common XML Schemas

## Authentication context parameters

This section defines the XML Schema for the <loacp:AuthContextParams> element present in the XML Schemas for LoA 1-4 above.

<xs:schema targetNamespace="http://id.elegnamnden.se/ns/1.0/loa-context-params"  
 xmlns:xs="http://www.w3.org/2001/XMLSchema"  
 xmlns="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <xs:element name="AuthContextParams" type="AuthContextParamsType"/>  
 <xs:complexType name="AuthContextParamsType">  
 <xs:sequence>  
 <xs:element maxOccurs="unbounded" minOccurs="1" ref="AuthContextParam"/>  
 </xs:sequence>  
 </xs:complexType>  
 <xs:element name="AuthContextParam" type="AuthContextParamType"/>  
 <xs:complexType name="AuthContextParamType">  
 <xs:simpleContent>  
 <xs:extension base="xs:string">  
 <xs:attribute name="Name" use="required" type="xs:string"/>  
 <xs:attribute name="ContentType" type="xs:string"/>  
 </xs:extension>  
 </xs:simpleContent>  
 </xs:complexType>  
 <xs:element name="Other" type="OtherType"/>  
 <xs:complexType name="OtherType">  
 <xs:sequence>  
 <xs:any maxOccurs="unbounded" minOccurs="0" namespace="##any" processContents="lax"/>  
 </xs:sequence>  
 </xs:complexType>  
</xs:schema>

Parameters that are included in authentication context class declarations in accordance with this schema is placed in <loacp:AuthContextParams> elements. The mandatory “Name” attribute defines conventions for interpretation of the element value as well as conventions of use of the optional “ContentType” attribute.

# References

[Eid2Tillit]

[Tillitsramverk för Svensk e-legitimation](http://www.elegnamnden.se/download/18.77dbcb041438070e039d237/1391026303972)

[SAML2AuthCont]

[Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, 15 March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf)

# Changes between versions

**Changes between version 1.0 and version 1.1:**

* Changes to all authentication context class definitions where they may now carry parameters.
* Chapter 3, “Common XML Schemas”, was added.