                Authentication Context Certificate Extension

Abstract

   This document defines an extension to X.509 certificates. The
   extension defined in this document holds data about how the
   certificate subject was authenticated by the Certification Authority
   that issued the certificate in which this extension appears.

   This document also defines one data structure for inclusion in this
   extension. The data structure is designed to hold information when
   the subject is authenticated using a Security Assertion Markup
   Language (SAML) assertion.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc7773.

Copyright Notice

Table of Contents

1. Introduction

   The primary purpose of this document is to provide a mechanism that
   allows an application to obtain information that expresses the
   identity of a subject in an X.509 certificate according to [RFC5280].
   The identity is stored either in a subject field attribute, as a
   subject alternative name, or in a subject directory attribute.

   The motivation for this work is to enable mapping of identity data
   between an identity system and a certificate where the identity
   system and the certificate are using different attributes and data
   formats to express the identity of the same entity. In such a
   scenario, the certificate subject already has an authenticated
   identity composed of a set of attributes, or so-called claims, that
   differ from the set of attributes that are commonly used to express
   the identity of a certificate subject and that may be governed by a
   specific certificate profile limiting that set.

   A typical scenario motivating the definition of this extension arises
   when the source of user authentication and user identity is derived
   from a SAML [SAML] federation attribute profile. In a SAML
   federation, the subject presents a SAML assertion in exchange for a
   certificate that can be uniquely linked to information provided in
   the original SAML assertion, e.g., attributes and/or level of
   assurance indicators.

Such certificates are sometimes issued in order to provide the user
with a means to create an electronic signature that ties the user to
the SAML subject, its attributes, and level of assurance indicators.

If such a certificate needs to conform to a certificate profile such
as [RFC3739], then this certificate may have to use a separate set of
attributes to express the subject identity. The certificate also may
have to employ a format for attribute values that is different from
the set of attributes obtained from the SAML assertion.

The extension defined in the document makes it possible to represent
information about the authentication context employed when
authenticating the subject for the purpose of issuing a certificate.
This may include information such as:

   o the Identity Provider that authenticated the subject
   o the level of assurance with which the subject was authenticated
   o the trust framework where this level of assurance was defined
   o a unique reference to the authentication instant
   o a mapping between the subject attributes (obtained from the
      SAML assertion used to authenticate the subject) and the
      subject identity information placed in the issued certificate.

One scenario where this information may be useful arises when a user
logs in to a service using SAML credentials, and the same user (at
some point) is required to sign some information. The service may
need to verify that the signature was created by the same user that
logged on to the service. Today this is only possible using out-of-
band knowledge about the Certification Authority (CA) that issued the
certificate and its practices. However, this approach does not scale
to a large number of service providers, identity providers, and CAs.

The extension defined here provides better scalability since it
requires only the service provider to maintain a list of trusted CAs.
All other information about the relationship between the certificate
subject and the SAML authenticated subject is available in the
certificate.

1.1. Terminology

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 RFC 2119 [RFC2119].

2. Authentication Context Extension Syntax

   The Authentication Context extension has the following syntax:

```
      AuthenticationContexts ::= SEQUENCE SIZE (1..MAX) OF
                                 AuthenticationContext

      AuthenticationContext ::= SEQUENCE {
          contextType     UTF8String,
          contextInfo     UTF8String OPTIONAL
      }
```

   This extension holds a sequence of AuthenticationContext information.
   When present, this extension MUST include at least one
   AuthenticationContext.

   The type of authentication context defined in AuthenticationContext
   is identified by the contextType. The contextType MUST contain a URI
   that identifies the context type as well as the data format and
   encoding of context information provided in contextInfo.

   This extension MAY be marked critical.

   Applications that find an authentication context information type
   they do not understand MUST ignore it if the extension is non-
   critical and MUST reject the certificate if the extension is marked
   critical. If an application requires that an authentication context
   exist, and either the extension is absent or none of the provided
   authentication contexts can be used, the end-user certificate fails
   validation.

   This document defines one authentication context information type
   (Section 3) that is used to provide information about SAML-based
   authentication of the subject that was utilized in the certificate
   issuance process. Other documents can define other authentication
   context information types.

3. SAML Authentication Context Information

   The SAML Authentication context information provides a contextType
   field that can be used to carry information about SAML-based
   authentication of the certified subject as utilized in the
   certificate issuance process.

The data carried in this authentication context information field is identified by the following XML schema ([Schema1] [Schema2]) name space:

    http://id.elegnamnden.se/auth-cont/1.0/saci

When this URI is specified as contextType, the associated XML data provided in contextInfo MUST be provided in the form of an XML document [XML], represented by a string of UTF-8-encoded characters.

The XML document SHOULD exclude any unnecessary line breaks and white space, such as line indentation, to reduce its size as much as possible.

3.1. contextInfo Data Structure

The data provided in contextInfo SHALL contain XML that is UTF-8 encoded in accordance with the XML schema provided in Appendix B. The XML document string in contextInfo MUST NOT include an XML header. That is, the XML document string contains only the root element <SAMLAuthContext> with its child elements <AuthContextInfo> and <IdAttributes>.

The <AuthContextInfo> and <IdAttributes> elements are outlined in the following subsections.

3.1.1. AuthContextInfo Element

The <AuthContextInfo> element MAY be present. This element contains the following attributes:

    IdentityProvider (required): The SAML EntityID of the Identity
       Provider that authenticated the subject.

    AuthenticationInstant (required): Date and time when the subject
       was authenticated, expressed according to Appendix B.1.

    AuthnContextClassRef (required): A URI identifying the
       AuthnContextClassRef that is provided in the AuthnStatement of
       the Assertion that was used to authenticate the subject. This
       URI identifies the context and the level of assurance
       associated with this instance of authentication.

    AssertionRef (optional): A unique reference to the SAML assertion.

    ServiceID (optional): An identifier of the service that verified
       the SAML assertion.

   The <AuthContextInfo> element may hold any number of child elements
   of type any (processContents="lax"), providing additional information
   according to local conventions. Any such elements SHOULD be ignored
   if not understood.

3.1.2. IdAttributes Element

   The <IdAttributes> element MAY be present. This element holds a
   sequence of one or more <AttributeMapping> elements, where each
   <AttributeMapping> element contains mapping information about one
   certificate subject attribute or name form present in the
   certificate.

   Each <AttributeMapping> element MUST specify the following
   attributes:

      Type: A string containing one of the enumerated values "rdn",
            "san", or "sda", specifying the type of certificate
            attribute or name form for which mapping information is
            provided:

               "rdn": Mapping information is provided for an attribute in
                      a Relative Distinguished Name located in the
                      subject field.
               "san": Mapping information is provided for a name in the
                      Subject Alternative Name extension of the
                      certificate.
               "sda": Mapping information is provided for an attribute in
                      the Subject Directory Attributes extension.

      Ref: A reference to the specific attribute or name field. This
            reference is dependent on the value of Type in the following
            way:

               "rdn": Ref holds a string representation of the object
                      identifier (OID) of the relative distinguished name
                      attribute.
               "san": Ref holds a string representation of the explicit
                      tag number of the Subject Alternative Name type
                      (e.g., "1" = email address (rfc822Name) and "2" =
                      dNSName). If the SubjectAlternative name is an
                      otherName, then Ref holds a string representation
                      of the OID defining the otherName form.
               "sda": Ref holds a string representation of the OID of the
                      subject directory attribute attribute.

String representations of object identifiers (OID) in the
Ref attribute MUST be represented by a sequence of integers
separated by a period, e.g., "2.5.4.32". This string
contains only numerals (ASCII 0x30 to 0x39) and periods
(ASCII 0x2E), and it MUST NOT contain any other characters.

Each <AttributeMapping> element MUST contain a <saml:Attribute>
element as defined in [SAML]. This SAML attribute element MUST have
a Name attribute (specifying its type), MAY have other attributes,
and MAY have zero or more <saml:AttributeValue> child elements. A
present SAML attribute with absent attribute value limits mapping to
the type of SAML attribute that was used to obtain the value stored
in the referenced certificate subject attribute or name form, without
duplicating the actual attribute value.

If an attribute value is present in the SAML attribute, then the
value stored in the certificate in the referenced attribute or name
form MAY differ in format and encoding from the present SAML
attribute value. For example, a SAML attribute value can specify a
country expressed as "Sweden", while this country value is stored in
the certificate in a countryName attribute using the two letter
country code "SE".

Several <AttributeMapping> elements MAY be present for the same
certificate subject attribute or name form if the certificate
contains multiple instances of this attribute or name form where
their values were obtained from different SAML attributes. However,
in such cases, it is not defined which present subject attribute or
name form maps to which SAML attribute. A certificate-using
application MAY attempt to determine this by comparing attribute
values stored in this extension with attribute or name values present
in the certificate, but this specification does not define any
explicit matching rules that would guarantee an unambiguous result.

The <AttributeMapping> element may hold any number of child elements
of type any (processContents="lax"), providing additional information
according to local conventions. Any such elements MAY be ignored if
not understood.

Note: The <AttributeMapping> element is designed to provide mapping
      between SAML attributes and certificate subject attributes and
      name forms where there is a distinct and clear relationship
      between relevant SAML attributes and corresponding certificate
      attributes and name forms. This does not cover all aspects of
      complex mapping situations. If more than one SAML attribute
      maps to the same certificate attribute or if structured
      multivalued attributes are split into a range of other
      attributes and name forms, these situations are not covered.

Such complex mapping situations MAY be covered by extending this XML schema or by defining a more versatile context information schema.

4. Security Considerations

This extension allows a CA to outsource the process used to identify and authenticate a subject to another trust infrastructure in a dynamic manner that may differ from certificate to certificate. Since the authentication context is explicitly declared in the certificate, one certificate may be issued with a lower level of assurance than another, even though both have the same Issuer.

This means that a relying party needs to be aware of the certificate policy under which this CA operates in order to understand when the certificate provides a level of assurance with regard to subject authentication that is higher than the lowest provided level. A relying party that is not capable of understanding the information in the authentication context extension MUST assume that the certificate is issued using the lowest allowed level of assurance declared by the policy.

5. Normative References

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3739]   Santesson, S., Nystrom, M., and T. Polk, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 3739, DOI 10.17487/RFC3739, March 2004, <http://www.rfc-editor.org/info/rfc3739>.

[RFC5280]   Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5912]   Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <http://www.rfc-editor.org/info/rfc5912>.

   [SAML]   Cantor, S., Kemp, J., Philpott, R., and E. Maler,
               "Assertions and Protocols for the OASIS Security Assertion
               Markup Language (SAML) V2.0", OASIS Standard, 15 March
               2005.

   [XML]   Bray, T., Paoli, J., Sperberg-McQueen, C., Maler, E., and
               F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth
               Edition)", W3C Recommendation, 26 November 2008,
               <https://www.w3.org/TR/2008/REC-xml-20081126/>.

   [Schema1]   Thompson, H., Beech, D., Maloney, M., and N. Mendelsohn,
               "XML Schema Part 1: Structures", W3C Recommendation,
               28 October 2004,
               <http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/>.

   [Schema2]   Biron, P. and A. Malhotra, "XML Schema Part 2: Datatypes",
               W3C Recommendation, 28 October 2004,
               <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>.

Appendix A. ASN.1 Modules

   This appendix includes the ASN.1 modules for the authentication
   context extension. Appendix B.1 includes an ASN.1 module that
   conforms to the 1998 version of ASN.1. Appendix B.2 includes an
   ASN.1 module, corresponding to the module present in Appendix B.1,
   that conforms to the 2008 version of ASN.1. Although a 2008 ASN.1
   module is provided, the module in Appendix B.1 remains the normative
   module as per policy adopted by the PKIX working group for
   certificate-related specifications.

A.1. ASN.1 1988 Syntax

```
 ACE-88
      {iso(1) member-body(2) se(752) e-legnamnden(201)
       id-mod(0) id-mod-auth-context-88(1)}

 DEFINITIONS EXPLICIT TAGS ::=

 BEGIN

 -- EXPORTS ALL --

 -- Authentication Context Extension

 AuthenticationContexts ::= SEQUENCE SIZE (1..MAX) OF
                            AuthenticationContext

 AuthenticationContext ::= SEQUENCE {
     contextType     UTF8String,
     contextInfo     UTF8String OPTIONAL
 }

 e-legnamnden       OBJECT IDENTIFIER ::= { iso(1) member-body(2)
                                    se(752) 201 }
 id-eleg-ce         OBJECT IDENTIFIER ::= { e-legnamnden 5 }
 id-ce-authContext OBJECT IDENTIFIER ::= { id-eleg-ce 1 }

 END
```

A.2. ASN.1 2008 Syntax

```
ACE-08
      {iso(1) member-body(2) se(752) e-legnamnden(201)
       id-mod(0) id-mod-auth-context-08(2)}

DEFINITIONS EXPLICIT TAGS ::=
BEGIN
EXPORTS ALL;
IMPORTS

Extensions{}, EXTENSION
FROM PKIX-CommonTypes-2009 -- From [RFC5912]
    {iso(1) identified-organization(3) dod(6) internet(1) security(5)
     mechanisms(5) pkix(7) id-mod(0) id-mod-pkixCommon-02(57)};

-- Authentication Context Extension

ext-AuthenticationContext EXTENSION ::= { SYNTAX
      AuthenticationContexts IDENTIFIED BY
      id-ce-authContext }

AuthenticationContexts ::= SEQUENCE SIZE (1..MAX) OF
                           AuthenticationContext

AuthenticationContext ::= SEQUENCE {
    contextType     UTF8String,
    contextInfo     UTF8String OPTIONAL
}

ElegnamndenCertExtensions EXTENSION ::= {
    ext-AuthenticationContext, ... }



e-legnamnden        OBJECT IDENTIFIER ::= { iso(1) member-body(2)
                                    se(752) 201 }
id-eleg-ce          OBJECT IDENTIFIER ::= { e-legnamnden 5 }
id-ce-authContext OBJECT IDENTIFIER ::= { id-eleg-ce 1 }

END
```

Appendix B. SAML Authentication Context Info XML Schema

  This appendix contains an XML schema ([Schema1] [Schema2]) for the SAML
  Authentication context information defined in Section 3.

  IMPORTANT NOTE: The XML Schema in Appendix B.1 specifies a URL on rows
                  9 and 10 to the SAML schemaLocation
                  (http://docs.oasis-open.org/security/saml/v2.0/
                  saml-schema-assertion-2.0.xsd), which is too long to
                  fit into one row and therefore contains a line break.
                  This line break has to be removed before this schema
                  can be successfully compiled.

B.1. XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           elementFormDefault="qualified"
     targetNamespace="http://id.elegnamnden.se/auth-cont/1.0/saci"
     xmlns:saci="http://id.elegnamnden.se/auth-cont/1.0/saci"
     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
         schemaLocation="http://docs.oasis-open.org/security/saml/v2.0/
 saml-schema-assertion-2.0.xsd"/>

     <xs:element name="SAMLAuthContext"
                 type="saci:SAMLAuthContextType"/>
     <xs:complexType name="SAMLAuthContextType">
         <xs:sequence>
             <xs:element ref="saci:AuthContextInfo" minOccurs="0"/>
             <xs:element ref="saci:IdAttributes" minOccurs="0"/>
         </xs:sequence>
     </xs:complexType>
     <xs:element name="AuthContextInfo"
                 type="saci:AuthContextInfoType"/>
     <xs:complexType name="AuthContextInfoType">
         <xs:sequence>
             <xs:any processContents="lax"
                 minOccurs="0" maxOccurs="unbounded"/>
         </xs:sequence>
         <xs:attribute name="IdentityProvider"
                       type="xs:string" use="required"/>
         <xs:attribute name="AuthenticationInstant"
                       type="xs:dateTime" use="required"/>
         <xs:attribute name="AuthnContextClassRef"
                       type="xs:anyURI" use="required"/>
         <xs:attribute name="AssertionRef" type="xs:string"/>
```

```
            <xs:attribute name="ServiceID" type="xs:string"/>
        </xs:complexType>

        <xs:element name="IdAttributes" type="saci:IdAttributesType"/>
        <xs:complexType name="IdAttributesType">
            <xs:sequence>
                <xs:element maxOccurs="unbounded" minOccurs="1"
                        ref="saci:AttributeMapping"/>
            </xs:sequence>
        </xs:complexType>
        <xs:element name="AttributeMapping"
                type="saci:AttributeMappingType"/>
        <xs:complexType name="AttributeMappingType">
            <xs:sequence>
                <xs:element ref="saml:Attribute"/>
                <xs:any processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attribute name="Type" use="required">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:enumeration value="rdn"/>
                        <xs:enumeration value="san"/>
                        <xs:enumeration value="sda"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:attribute>
            <xs:attribute name="Ref" type="xs:string" use="required"/>
        </xs:complexType>
    </xs:schema>
```

Appendix C. SAML Authentication Context Info XML Examples

   This appendix provides examples of SAML Authentication Context
   information according to the schema in Appendix B.

C.1. Complete Context Information and Mappings

   The following is a complete example with authentication context
   information as well as mapping information for several subject field
   attributes and a subject alt name.

```
<saci:SAMLAuthContext
    xmlns:saci="http://id.elegnamnden.se/auth-cont/1.0/saci"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saci:AuthContextInfo
        ServiceID="eid2csig"
        AssertionRef="_71b981ab017eb42869ae4b62b2a63add"
        IdentityProvider="https://idp-test.nordu.net/idp/shibboleth"
        AuthenticationInstant="2013-03-05T22:59:57.000+01:00"
        AuthnContextClassRef="http://id.elegnamnden.se/loa/1.0/loa3"/>
    <saci:IdAttributes>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.6">
            <saml:Attribute
                FriendlyName="Country"
                Name="urn:oid:2.5.4.6">
                <saml:AttributeValue xsi:type="xs:string"
                    >SE</saml:AttributeValue>
            </saml:Attribute>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.5">
            <saml:Attribute
                FriendlyName="Personal ID Number"
                Name="urn:oid:1.2.752.29.4.13">
                <saml:AttributeValue xsi:type="xs:string"
                    >200007292386</saml:AttributeValue>
            </saml:Attribute>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.42">
            <saml:Attribute
                FriendlyName="Given Name"
                Name="urn:oid:2.5.4.42">
                <saml:AttributeValue xsi:type="xs:string"
                    >John</saml:AttributeValue>
            </saml:Attribute>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.4">
            <saml:Attribute
```

```
                    FriendlyName="Surname"
                    Name="urn:oid:2.5.4.4">
                    <saml:AttributeValue xsi:type="xs:string"
                        >Doe</saml:AttributeValue>
                </saml:Attribute>
            </saci:AttributeMapping>
            <saci:AttributeMapping Type="rdn" Ref="2.5.4.3">
                <saml:Attribute
                    FriendlyName="Display Name"
                    Name="urn:oid:2.16.840.1.113730.3.1.241">
                    <saml:AttributeValue xsi:type="xs:string"
                        >John Doe</saml:AttributeValue>
                </saml:Attribute>
            </saci:AttributeMapping>
            <saci:AttributeMapping Type="san" Ref="1">
                <saml:Attribute
                    FriendlyName="E-mail"
                    Name="urn:oid:0.9.2342.19200300.100.1.3">
                    <saml:AttributeValue xsi:type="xs:string"
                        >john.doe@example.com</saml:AttributeValue>
                </saml:Attribute>
            </saci:AttributeMapping>
        </saci:IdAttributes>
</saci:SAMLAuthContext>
```

C.2. Only Mapping Information without SAML Attribute Values

   This example shows an instance of the SAML Authentication Context
   information that only provides a mapping table without providing any
   authentication context information or SAML attribute values.

```
<saci:SAMLAuthContext
    xmlns:saci="http://id.elegnamnden.se/auth-cont/1.0/saci"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <saci:IdAttributes>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.6">
            <saml:Attribute Name="urn:oid:2.5.4.6"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.5">
            <saml:Attribute Name="urn:oid:1.2.752.29.4.13"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.42">
            <saml:Attribute Name="urn:oid:2.5.4.42"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.4">
            <saml:Attribute Name="urn:oid:2.5.4.4"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.3">
```

```
            <saml:Attribute Name="urn:oid:2.16.840.1.113730.3.1.241"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="san" Ref="1">
            <saml:Attribute Name="urn:oid:0.9.2342.19200300.100.1.3"/>
        </saci:AttributeMapping>
    </saci:IdAttributes>
</saci:SAMLAuthContext>
```

C.3. Authentication Context and serialNumber Mapping

This example shows an instance of the SAML Authentication Context information; it provides authentication context information and mapping information that specifies the source of the data stored in the serialNumber attribute in the subject field.

```
<saci:SAMLAuthContext
    xmlns:saci="http://id.elegnamnden.se/auth-cont/1.0/saci"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saci:AuthContextInfo
        ServiceID="eid2csig"
        AssertionRef="_71b981ab017eb42869ae4b62b2a63add"
        IdentityProvider="https://idp-test.nordu.net/idp/shibboleth"
        AuthenticationInstant="2013-03-05T22:59:57.000+01:00"
        AuthnContextClassRef="http://id.elegnamnden.se/loa/1.0/loa3"/>
    <saci:IdAttributes>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.5">
            <saml:Attribute
                FriendlyName="Personal ID Number"
                Name="urn:oid:1.2.752.29.4.13">
                <saml:AttributeValue xsi:type="xs:string"
                    >200007292386</saml:AttributeValue>
            </saml:Attribute>
        </saci:AttributeMapping>
    </saci:IdAttributes>
</saci:SAMLAuthContext>
```

Author's Address

Stefan Santesson
3xA Security AB
Scheelev. 17
223 70 Lund
Sweden
Email: sts@aaa-sec.com