INTERNET-DRAFT
Intended Status: Informational
Expires: August 17, 2013

Stefan Santesson
(3xA Security)

February 13, 2013

Authentication Context Certificate Extension
draft-santesson-auth-context-extension-02

Abstract

This document defines an extension to certificates according to [RFC5280]. The extension defined in this document holds data about how the certificate subject was authenticated by the Certification Authority who issued the certificate where this extension appears.

This document also defines one data structure for inclusion in this extension that designed to hold information when the subject is authenticated using a SAML assertion [SAML].

Status of this Memo

Copyright and License Notice

Table of Contents

1 Introduction

This document addresses some needs that may arise when issuing a certificate from an existing non-certificate based identity infrastructure where the certificate subject already has an authenticated identity composed of a set of attributes, or so called claims, that differ from the attributes that are commonly used to express the identity of a certificate subject.

A typical scenario for this is when the basic trust infrastructure is based on a SAML federation, where the subject for some reason needs a certificate that can be traced back to that subjects SAML credentials, both with regard to identity and with regard to level of assurance with which the subject has been authenticated.

A reason to issue such certificate may arise if the subject needs a certificate to support signing a document, where the Certification Authority is authenticating the user by means of the SAML federation when issuing that signature certificate.

If that signature certificate need to conform to certificate profiles, such as [RFC3739], then this certificate may have to use a separate set of attributes to express the subject identity than the set of attributes obtained from the SAML assertion.

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

- The Identity Provider which authenticated the subject.
- The level of assurance with which the subject was authenticated.
- The trust framework where this level of assurance was defined.
- A unique reference to the authentication instant
- A mapping table 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 is when a user logs in to a service using SAML credentials, where the same user at some stage 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. This is only possible today using out-of-band knowledge about the CA that issued the certificate and it's practices. This is is however hard to scale and maintain using a large number of service providers, identity providers and CAs.

The defined extension provides better scalability since it only requires the service provider to maintain a list of trusted CA:s. All other information abut 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].

1.2 Deployment

EDITORS NOTE:

[This section provided information for better understanding the rationale of the extension. This section can be deleted is the document is published]

The extension defined in this draft has been defined and deployed in the National Swedish Identity infrastructure Eid 2.0 which is based on SAML federated identity. The Swedish infrastructure will go live during 2013 and will provide secure identification of citizens in Swedish government services. A central requirement in these government services is to allow citizens to sign various documents, representing a wide range of declarations and applications.

A central part of this infrastructure is therefore to use centralized signature services that allows citizens to sign using their SAML credentials. As service providers authenticate and understands user identities only under a SAML context within this national infrastructure, this extension allows Service Providers to determine whether a presented signature matches a particular user and whether it meets the security requirements of the service.

Through information provided in this extension a service provider may for example get notice that the user logged on using one level of assurance, but presented a signature which certificate was issued using a certificate obtained using a lower level of assurance procedure, and thus reject the signature.

This extension is therefore fundamental to the function of the Swedish Eid 2.0 infrastructure.

2. Authentication Context Extension Syntax

The Authentication Context extension has the following syntax:

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

AuthenticationContext ::= SEQUENCE {
    contextType   OBJECT IDENTIFIER,
    mimeType        PrintableString OPTIONAL,
    contextInfo   OCTET STRING
}
```

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

The type of authentication context information included in AuthenticationContext is identified by the contextType object identifier. The authentication context information is carried in contextInfo using a data format that is identified by the specified mimeType.

If mimeType is absent, then contextInfo MUST hold a DER encoded ASN.1 structure.

This document defines one authentication context information type identified by the contextType object identifier (Section 3) that is used to provide information about SAML based authentication. Other documents can define other authentication context information types. Each information type MUST define both data format and structure of the data stored in contextInfo.

Applications which find an authentication context information type they do not understand MUST ignore it. 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 MUST fail validation of the end user certificate.

This extension MAY be marked critical.

3 SAML Authentication Context Information

The SAML Authentication context information provides a contextType type that can be used to carry information about SAML based authentication of the certified subject as part of the certificate issuing process.

The data carried in this authentication context information type is provided in JSON format, identified by the following mime type:

```
application/json
```

This data structure is identified by the contextType Object Identifier id-ct-saml-ac.

```
id-ct-saml-ac     OBJECT IDENTIFIER ::= { id-eleg-ct 1}
```

The JSON data format is used mainly to allow this context information to be extracted and processed in applications that lacks ASN.1 processing capabilities. JSON is easy to deserialize into various data objects both in application and web environments for further comparison with the characteristics of SAML authenticated sessions.

The data provided in contextInfo SHALL be the byte representation of an UTF-8 encoded string holding JSON formatted data in accordance with Appendix B. The content of the two JSON objects authContextInfo and idAttributes are outlined in the following subsections.

3.1   authContextInfo object

The authContextInfo object MAY be present in the statement. When present, the following conventions SHALL apply to the parameters carried in the authContext object:

identityProvider   (required): The SAML EntityID of the Identity Provider which authenticated the subject.

authenticationInstant (required): Date and time when the subject was authenticated.

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 arbitrary identifier of the service that verified the SAML assertion.

3.2 idAttributes object

The idAttributes object MAY be present in the statement. When present, this object holds an array of attribute statements, where each object in the array holds information about one SAML attribute value that was included in the certificate as a representation of the certified subject.

When present, each attribute statement SHALL comply with the following conventions:

name (Optional): An arbitrary friendly name of the attribute.

samlAttr (Required): A URI identifying the SAML attribute that contained the value in attrVlaue.

attrValue (Required): The attribute value carried in the SAML attribute.

certNameType (Required): A string holding one of the enumerated values "rdn", "san" or "sda", having the following meaning:

- "rdn" The attribute value is placed in the subject field of the certificate in a present Relative Distinguished Name attribute.
- "san" The attribute value is placed in the Subject Alternative Name extension of the certificate.
- "sda" The attribute value is stored an a Subject Directory Attributes extension.

certRef (Required): A reference to the corresponding attribute or name field where the attribute value is stored in the certificate. The certRef holds a string value which is dependent on the value of certNameType. The value of certRef MUST contain the following information when the value of certNameType is;

- "rdn" A string representation of the OID of the attribute that holds the corresponding attribute value in the subject field.
- "sda" A string representation of the OID of the attribute that holds the corresponding attribute value in the subject directory attributes extension.
- "san" A string representation of the explicit tag number of the Subject Alternative Name

type (e.g. "1" = e-mail address (rfc822Name) and "2" = dNSName). If the SubjectAlternative name is an otherName, then the certRef holds a string representation of the OID defining the otherName form.

String representations of object identifiers (OID) MUST be represented by a sequence of integers separated by a period. E.g. "2.5.4.32". This string MUST NOT contain any white-space or line breaks.

The SAML attributes name (in samlAttr) is represented in URI form as defined in the [SAML] standard. This URI MAY express an OID. When this parameter holds an OID it MUST be represented by a string that starts with "urn:oid:" and ends with a string representation of the OID (e.g. "urn:oid:2.5.4.42").

3 Security Considerations

This extension allows a CA to outsource the process to identify and authenticate a subject to another trust infrastructure in a dynamic manner that may differ form 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.

This means that the relying party need 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.

4 IANA Considerations

This document contains no actions for IANA.

5 References

5.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3739] Santesson, S., Nystrom, M., and T. Polk, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 3739, March 2004.

[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, May 2008.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, June 2010.

[SAML] Scot Cantor, John Kemp, Rob Philpott, Eve Maler, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005

5.2 Informative References

[JSON-SCHEMA] F. Galiegue, K. Zyp, "JSON Schema: core definitions and terminology", draft-zyp-json-schema-04, January 31, 2013.

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 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

IMPORTS

-- Certificate Extensions

   Extensions
   FROM PKIX1Explicit88 { iso(1) identified-organization(3)
        dod(6) internet(1) security(5) mechanisms(5) pkix(7)
        id-mod(0) id-pkix1-explicit(18) };


-- Authentication Context Extension

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

AuthenticationContext ::= SEQUENCE {
    contextType   OBJECT IDENTIFIER,
    mimeType     PrintableString OPTIONAL,
    contextInfo   OCTET STRING
}
```

```
 e-legnamnden      OBJECT IDENTIFIER ::= { iso(1) member-body(2)
                                           se(752) 201 }
 id-eleg-ce        OBJECT IDENTIFIER ::= { e-legnamnden 5 }
 id-eleg-ct        OBJECT IDENTIFIER ::= { e-legnamnden 6 }
 id-ce-authContext OBJECT IDENTIFIER ::= { id-eleg-ce 1 }
 id-ct-saml-ac     OBJECT IDENTIFIER ::= { id-eleg-ct 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
 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)}

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

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

 AuthenticationContext ::= SEQUENCE {
     contextType   OBJECT IDENTIFIER {{id-ct-saml-ac,...}},
     mimeType     PrintableString OPTIONAL,
     contextInfo   OCTET STRING
 }


 e-legnamnden      OBJECT IDENTIFIER ::= { iso(1) member-body(2)
                                           se(752) 201 }
 id-eleg-ce        OBJECT IDENTIFIER ::= { e-legnamnden 5 }
 id-eleg-ct        OBJECT IDENTIFIER ::= { e-legnamnden 6 }
 id-ce-authContext OBJECT IDENTIFIER ::= { id-eleg-ce 1 }
 id-ct-saml-ac     OBJECT IDENTIFIER ::= { id-eleg-ct 1}


 END
```

Appendix B - SAML Authentication Context Data Structures

This appendix includes data structure definitions for the SAML Authentication context information defined in section 3.

Data structure definitions using JSON schema [JSON-SCEMA] is provided in B.1 and a corresponding definition using Java Classes is provided in B.2. As the JSON schema currently is in draft form the definitions provided B.2 is the normative one.

B.1 JSON Schema

```
 {
     "type": "object",
     "$schema": "http://json-schema.org/schema#",
     "required": false,
     "properties": {
         "authContextInfo": {
             "description": "SAML Authentication Context Information",
             "type": "object",
             "required": false,
             "properties": {
                 "identityProvider": {
                     "type": "string",
                     "required": true
                 },
                 "authenticationInstant": {
                     "type": "date-time",
                     "required": true
                 },
                 "authnContextClassRef": {
                     "type": "string",
                     "required": true
                 },
                 "assertionRef": {
                     "type": "string",
                     "required": false
                 },
                 "serviceID": {
                     "type": "string",
                     "required": false
                 }
             }
         },
         "idAttributes": {
             "description": "Information about subject attributes",
             "type": "array",
             "required": false,
```

```
             "items": {
                 "type": "object",
                 "required": false,
                 "properties": {
                     "name": {
                         "type": "string",
                         "required": false
                     },
                     "samlAttr": {
                         "type": "string",
                         "required": true
                     },
                     "attrValue": {
                         "type": "string",
                         "required": true
                     },
                     "certNameType": {
                         "type": "string",
                         "enum": [
                             "rdn",
                             "san",
                             "sda"
                         ],
                         "required": true
                     },
                     "certRef": {
                         "type": "string",
                         "required": true
                     }
                 }
             }
         }
     }
 }
```

B.2 JAVA Class Declaration

This section defines the content of the SAML Authentication Context data structure using Java Syntax. The JSON string is obtained by serializing an object of the class SAMLAuthContext to JSON.

These Java classes only defines structure, but not whether a particular element is mandatory or optional. Requirements on mandatory or optionally elements is provided in section 3 as well as in the JSON schema provided in section B.1.

```
  class SAMLAuthContext {
      AuthContextInfo authContextInfo;
```

```
        IdAttributes[] idAttributes;
    }

    class AuthContextInfo {
        String identityProvider;
        Date authenticationInstant;
        String authnContextClassRef;
        String assertionRef;
        String serviceID;
    }

    class IdAttributes {
        String name;
        String samlAttr;
        String attrValue;
        CertNameType certNameType;
        String certRef;
    }

    enum CertNameType {
        rdn, san, sda;
    }
```

B.2 Example

```
{
  "authContextInfo": {
    "identityProvider": "https://idp.example.com/shibboleth",
    "authenticationInstant": "Feb 12, 2013 12:34:47 AM",
    "authnContextClassRef":
    "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
    "assertionRef": "_e774ccf2b68ae4324f4ed565bcb9af40",
    "serviceID": "ca.example.com"
  },
  "idAttributes": [
    {
      "name": "Given Name",
      "samlAttr": "urn:oid:2.5.4.42",
      "attrValue": "John",
      "certNameType": "rdn",
      "certRef": "2.5.4.42"
    },
    {
      "name": "Surname",
      "samlAttr": "urn:oid:2.5.4.4",
      "attrValue": "Doe",
      "certNameType": "rdn",
```

```
      "certRef": "2.5.4.4"
    },
    {
      "name": "Swedish Personnummer",
      "samlAttr": "urn:oid:1.2.752.29.4.13",
      "attrValue": "200007292386",
      "certNameType": "rdn",
      "certRef": "2.5.4.5"
    },
    {
      "name": "E-mail",
      "samlAttr": "urn:oid:0.9.2342.19200300.100.1.3",
      "attrValue": "john.doe@example.com",
      "certNameType": "san",
      "certRef": "1"
    }
  ]
}
```

Authors' Addresses

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