SAML V2.0 Holder-of-Key AsserSubject Confirmation Profile

Working Draft 02, 141, 7 August 2008

Specification URIs:
TBD

Technical Committee:
OASIS Security Services TC

Chair(s):
Hal Lockhart, BEA Systems, Inc.
Brian Campbell, Ping Identity Corporation

Editors:
Tom Scavo, National Center for Supercomputing Applications (NCSA)

Contributors:
Nate Klingenstein, Internet2
Scott Cantor, Internet2

Abstract:
This profile describes the issuing and processing of a holder-of-key `<saml:SubjectConfirmation>` element. Specifically, we show how an identity providerSAML issuer binds X.509 data to a `<ds:KeyInfo>` element and how a service providerrelying party confirms that a `<ds:KeyInfo>` element matches given X.509 data. The binding material used by the identity providerSAML issuer and the matching data used by the service providerrelying party is obtained from a standard X.509 public key certificate.

Status

This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC by using the "Send A Comment" button on the TC's web page at http://www.oasis-open.org/committees/security.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the IPR section of the TC web page (http://www.oasis-open.org/committees/security/ipr.php).

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

This *SAML V2.0 Holder-of-Key ~~Subject Confirmation~~Assertion Profile* describes the issuing and processing of a holder-of-key `<saml:SubjectConfirmation>` element. Specifically, we show how a~~n identity provider~~SAML issuer binds X.509 data to a `<ds:KeyInfo>` element and how a~~n service provider~~relying party confirms that a `<ds:KeyInfo>` element matches given X.509 data. The binding material used by the ~~identity provider~~SAML issuer and the matching data used by the ~~service provider~~relying party is obtained from a standard X.509 public key certificate.

A distinguishing characteristic of this profile is that *the presenter is the subject*. The case where the presenter is acting on behalf of the subject does not apply since the latter does not result in holder-of-key SAML assertions.

1.1 Notation

This specification uses normative text.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC2119]:

> …they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)…

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

```
Listings of XML schemas appear like this.
```

```
Example code listings appear like this.
```

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

Prefix	XML Namespace	Comments
`saml:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].
`ds:`	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace [XMLSig].
~~Prefix~~	~~XML Namespace~~	~~Comments~~
~~`saml:`~~	~~urn:oasis:names:tc:SAML:2.0:assertion~~	~~This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].~~
~~`samlp:`~~	~~urn:oasis:names:tc:SAML:2.0:protocol~~	~~This is the SAML V2.0 protocol namespace defined in the SAML V2.0 core specification [SAML2Core].~~
~~`ds:`~~	~~http://www.w3.org/2000/09/xmldsig#~~	~~This is the XML Signature namespace [XMLSig].~~

This specification uses the following typographical conventions in text: `<SAMLElement>`, `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherCode`.

1.2 Normative References

[RFC2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC2253] M. Wahl, S. Kille, T. Howes. *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names.* IETF RFC 2253, December 1997. http://www.ietf.org/rfc/rfc2253.txt

[SAML2Core] S. Cantor, J. Kemp, R. Philpott, E. Maler. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2Prof] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, P. Mishra, R. Philpott, E. Maler. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[XMLSig] D. Eastlake, J. Reagle, D. Solo. *XML-Signature Syntax and Processing.* World Wide Web Consortium Recommendation, 12 February 2002. http://www.w3.org/TR/xmldsig-core/

1.3 Non-normative References

[AIXCM] T. Moreau. *Auto Issued X.509 Certificate Mechanism (AIXCM).* IETF Internet-Draft, 6 August 2008. See http://www.ietf.org/internet-drafts/draft-moreau-pkix-aixcm-00.txt~~**CONNOTECH]** T. Moreau. *Explicit Meaningless X.509 Security Certificates as a Specifications-Based Interoperability Mechanism.* CONNOTECH Document Number C004635 (2008/07/23). http://www.connotech.com/pkc-only-meaningless-certs.pdf~~

[RFC3820] S. Tuecke, V. Welch, D. Engert, L. Pearlman, M. Thompson. *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile.* IETF RFC 3820, June 2004. http://www.ietf.org/rfc/rfc3820.txt

[RFC4346] T. Dierks, E. Rescorla. *The Transport Layer Security (TLS) Protocol.* IETF RFC 4346, April 2006. http://www.ietf.org/rfc/rfc4346.txt

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* IETF RFC 5280, May 2008. http://www.ietf.org/rfc/rfc5280.txt

1.4 Conformance

1.4.1 SAML V2.0 Holder-of-Key Asser~~Subject Confirma~~tion Profile

All parties involved MUST conform to section 2.3. This includes the ~~identity provider~~SAML issuer, the ~~service provider~~relying party, and the ~~presenter~~subject.

A~~n identity provider~~SAML issuer MUST follow the issuing rules in section 2.4. In particular, a~~n identity provider~~SAML issuer MUST produce `<ds:KeyInfo>` elements that conform to section 2.4.1. Likewise, a ~~service provider~~relying party MUST follow the processing rules in section 2.5.

To claim conformance to this specification, a~~n identity provider~~SAML issuer implementation MUST support both the `<ds:X509Certificate>` element and the `<ds:X509SKI>` element specified in section 2.4.1. Support for the `<ds:X509SubjectName>` element and the `<ds:X509SerialIssuer>` element by SAML issuers~~identity providers~~ is OPTIONAL.

Likewise a conforming ~~service provider~~relying party implementation MUST support both the `<ds:X509Certificate>` element and the `<ds:X509SKI>` element specified in section 2.5. Support for

the <ds:X509SubjectName> element and the <ds:X509SerialIssuer> element by relying parties~~service providers~~ is OPTIONAL.

2 SAML V2.0 Holder-of-Key AsserSubject Confirmation Profile

2.1 Required Information

Contact information: security-services-comment@lists.oasis-open.org

SAML Confirmation Method Identifiers: The SAML V2.0 holder-of-key confirmation method identifier (`urn:oasis:names:tc:SAML:2.0:cm:holder-of-key`) is associated with every `<saml:SubjectConfirmation>` element issued under this profile.

Description: Given below.

Updates: RefinesExtends the holder-of-key confirmation method described in section 3.1 of [SAML2Prof].

2.2 Background

A distinguishing characteristic of this profile is that *the presenter is the subject*. The case where the presenter is acting on behalf of the subject does not apply since the latter does not result in holder-of-key SAML assertions.

Suppose a presentersubject presents a SAML request and an X.509 certificate to a SAML identity provideriissuer. The presentersubject proves possession of the private key corresponding to the public key of the presented certificate and authenticates to the SAML issueridentity provider by unspecified means. The SAML issueridentity provider consumes the SAML request and returns a SAML response to the presentersubject.

Assume the SAML response issued by the SAML issueridentity provider contains one or more holder-of-key assertions (otherwise this specification is not applicable). By definition, a *holder-of-key SAML assertion* contains a `<saml:SubjectConfirmation>` element whose `Method` attribute is set to `urn:oasis:names:tc:SAML:2.0:cm:holder-of-key`. This specification describes how the identity providerSAML issuer binds selected X.509 data to the `<saml:SubjectConfirmation>` element of a holder-of-key assertion.

The complementary exchange involves a presentersubject who presents a signed holder-of-key SAML assertion and an X.509 certificate to a SAML service providerrelying party. Again the presentersubject proves possession of the private key corresponding to the public key of the presented certificate, after which the service providerrelying party consumes the assertion and creates a security context for the subject. This specification describes how the service providerrelying party confirms that the X.509 data bound to the assertion matches the data in the X.509 certificate.

For the purposes of this profile, the particular binding used at the protocol layer is unspecified. The holder-of-key assertion may be bound to the original SAML response in a complete end-to-end flow, or the response may be consumed at some intermediate step, leaving the assertion to be bound to something else such as a SOAP header or perhaps even the X.509 certificate itself. In any event, it's the assertion that's of interest in the subsequent exchange, not the binding substrate.

We assume that the service providerrelying party trusts the identity providerSAML issuer to issue assertions regarding the subject. On the other hand, the identity providerSAML issuer may not even know the intended service providerrelying party (if the presentersubject is the SAML requester, e.g.), so there is no underlying assumption that the identity providerSAML issuer trusts the service providerrelying party.

The identity providerSAML issuer and the service providerrelying party may or may not trust the issuer of the X.509 certificate. For our purposes here, this is mostly out of scope. In some situations, however, it is assumed that the service providerrelying party trusts the X.509 issuer to safely confirm the subject. These

cases are included for completeness but a conforming SAML entity (~~identity provider~~issuer or ~~service provider~~relying party) is not mandated to implement these special cases.

2.3 X.509 Certificate Usage

There are no explicit requirements with respect to the X.509 certificate presented to the ~~identity provider~~SAML issuer, and later to the ~~service provider~~relying party. All that matters is that the ~~presenter~~subject MUST prove possession of the private key corresponding to the presented public key. The fact that the latter is typically bound to an X.509 public key certificate is mostly irrelevant.

That said, this specification mandates that the ~~presenter~~subject MUST present an X.509 public key certificate ~~[RFC5280]~~ to the ~~identity provider~~SAML issuer or the ~~service provider~~relying party. However, the specific characteristics of this certificate are wholly out of scope with respect to this specification. In particular, there is no expectation that either the ~~identity provider~~SAML issuer or the ~~service provider~~relying party trusts the issuer of the certificate, and therefore all portions of the certificate, apart from the public key, are out of scope.

The only exception is the case where the `<ds:X509Data>` element specified in section 2.4.1 contains a `<ds:X509SubjectName>` element or a `<ds:X509SerialIssuer>` element. In these two cases, the ~~service provider~~relying party MUST trust the X.509 issuer in order to confirm the subject. This is discussed more fully in section 2.5 below.

2.4 Holder-of-Key Subject Confirmation Issuing Rules

Every assertion containing a holder-of-key `<saml:SubjectConfirmation>` element MUST conform to [SAML2Core] (see section 2.4.1, and especially section 2.4.1.3) and section 3.1 of [SAML2Prof]. Where this specification conflicts with the SAML V2.0 specification, the former takes precedence.

The ~~presenter~~subject presents a SAML request and an X.509 certificate to the ~~identity provider~~SAML issuer. The ~~presenter~~subject MUST prove possession of the private key corresponding to the public key of the presented certificate. The ~~presenter~~subject authenticates to the ~~identity provider~~SAML issuer by unspecified means.

If the ~~presenter~~subject can prove possession of the private key, the ~~identity provider~~SAML issuer issues a response containing one or more holder-of-key assertions. The expected content of a holder-of-key `<saml:SubjectConfirmation>` element is specified in the next section~~`<samlp:Response>` element containing one or more holder-of-key assertions. If the presenter is unable to prove possession of the private key, or the identity provider wishes to return an error for any other reason, the identity provider MUST NOT include any assertions in the `<samlp:Response>` message. Otherwise the `<samlp:Response>` element MUST contain at least one holder-of-key assertion. Each holder-of-key assertion MUST be signed. The `<samlp:Response>` element MAY itself be signed~~.

~~The expected content of a holder-of-key `<saml:SubjectConfirmation>` element is specified in the next section.~~

2.4.1 KeyInfo Usage

According to the SAML V2.0 specification, a holder-of-key `<saml:SubjectConfirmation>` element MUST contain at least one `<ds:KeyInfo>` element, and that `<ds:KeyInfo>` element MUST conform to the XML Signature specification [XMLSig]. The current specification further constrains the content of each `<ds:KeyInfo>` element to contain exactly one `<ds:X509Data>` element. The `<ds:X509Data>` element MUST NOT contain a `<ds:X509CRL>` element. Instead, the following content options are specified, at least one of which MUST be satisfied:

- The <ds:X509Data> element MAY contain a <ds:X509Certificate> element. If it does, the <ds:X509Certificate> element MUST contain a base64 encoding of the DER-encoded X.509 certificate presented to the ~~identity provider~~SAML issuer.

- The <ds:X509Data> element MAY contain a <ds:X509SKI> element. If it does, the <ds:X509SKI> element MUST contain a base64 encoding of the SHA-1 hash of the public key bound to the X.509 certificate presented to the ~~identity provider~~SAML issuer.

- The <ds:X509Data> element MAY contain a <ds:X509SubjectName> element. If it does, the <ds:X509SubjectName> element MUST contain the subject distinguished name (DN) bound to the X.509 certificate presented to the ~~identity provider~~SAML issuer.

- The <ds:X509Data> element MAY contain a <ds:X509IssuerSerial> element. If it does, the <ds:X509IssuerSerial> element MUST contain the issuer DN and the issuer serial number (as specified in [XMLSig]) bound to the X.509 certificate presented to the ~~identity provider~~SAML issuer.

Use of the <ds:X509Certificate> element or the <ds:X509IssuerSerial> element is most restrictive since the exact same certificate must be presented to both the ~~identity provider~~SAML issuer and the ~~service provider~~relying party. Use of the <ds:X509SKI> element or the <ds:X509SubjectName> element is less restrictive since a different certificate may be presented to the ~~service provider~~relying party provided the certificate contains the same key or DN (resp.) presented to the ~~identity provider~~SAML issuer.

Use of the <ds:X509SubjectName> element or the <ds:X509IssuerSerial> element is warranted in those situations where the ~~service provider~~relying party trusts the issuer of the X.509 certificate. The ~~identity provider~~SAML issuer SHOULD NOT bind either of these elements to the <ds:X509Data> element unless it knows such a trust relationship exists.

Note that the format of the DN contained in the <ds:X509SubjectName> element or the <ds:X509IssuerSerial> element is specified in [XMLSig]. It is RECOMMENDED that the DN conform to [RFC2253] in all cases.

2.4.2 Example

Here is an example of a holder-of-key <saml:SubjectConfirmation> element containing both a <ds:X509Certificate> element and a <ds:X509SKI> element:

```
<saml:SubjectConfirmation
  Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
  <saml:SubjectConfirmationData
    Address="141.142.234.158"
    InResponseTo="someId1218218187577"
    NotOnOrAfter="2008-08-08T18:01:27.712Z"
    Recipient="https://useragent.example.org">
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>
MIIDuDCCAqACCQCJZK8wF0xVXjANBgkqhkiG9w0BAQQFADCBnTELMAkGA1UEBhMCQlIxEzARBgNV
BAgTClNvbWUtU3RhdGUxEjAQBgNVBAcTCVNvbWUtQ2l0eTESMBAGA1UEChMJR1NvQyAyMDA4MRIw
EAYDVQQLEwlHU29DIDIwMDgxFzAVBgNVBAMTDkpvYW5hIFRyaW5kYWRlMSQwIgYJKoZIhvcNAQkB
FhVzb21lLWFkZHJlc3NAaG9zdC5vcmcwHhcNMDgwNjE2MTcyMTQzWhcNMDkwNjE2MTcyMTQzWjCB
nTELMAkGA1UEBhMCQlIxEzARBgNVBAgTClNvbWUtU3RhdGUxEjAQBgNVBAcTCVNvbWUtQ2l0eTES
MBAGA1UEChMJR1NvQyAyMDA4MRIwEAYDVQQLEwlHU29DIDIwMDgxFzAVBgNVBAMTDkpvYW5hIFRy
aW5kYWRlMSQwIgYJKoZIhvcNAQkBFhVzb21lLWFkZHJlc3NAaG9zdC5vcmcwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDIDVKdO2CCVYA0TspOPmcSNnivjQq7jCacrqRPawKi3/pTuvnW
3c2XCpyT2s6Sks3Eq5T4HIXta5E+lOpN8VbTunVdSrac54r2uK8x+8AqX7M0wQw+98iGw9E2an5q
xRZfqqE1T5jWL/a/G1/e2TGlmp521W3k1nNtf8rYH39JpwBSZMeW7uHOSZOkT/pVvqPTgG7vUQT6
BiRh7PfwsLrLOMubbeQ6Z2m3Vnsv20E1FbPzwswzh4X1qXj9bnyI2UsuoisW9Y4p4byjL3GJ/hxp
mjRjXs+aIpzi0V3MH+jVJ98eomhlUFLaE83xycC8lns+FcCSQZ8RsbnaLZrtC8r7AgMBAAEwDQYJ
KoZIhvcNAQEEBQADggEBACwnWSEpwq5aE7QBdDNNXyok34RIonYi9690yw7i+JU7R/QdE42GERJS
```

```
DVKBN959ELLJf5d0vybGv08QWbZVQ7eBGn9xaZ7MhSnblYNDXs9vuv1V2Dy32q1J5nCSzqpJDyln
lVFWe9UQMCJOO6ibUtWLhiDQ49kmMabgyYfX28qB6oRdVL+mDI/XTt+mkCgk4Rs78n4kbX6qnRlj
dE/YnibP1A7iMh8pQkv49J6sP9SeUmQ2zxKCt3tSRzzypWc8JjOZGuBYGQHl9Xm7WEs4CXS7iZJW
E32frMAtavMcTM/qnDtCc8tZAxl2PSLOF1954vapfMjBhq3VTI6QRW//wPE=
          </ds:X509Certificate>
          <ds:X509SKI>YphoxnLNAx/S0sdbdN3nD01wuR8=</ds:X509SKI>
       </ds:X509Data>
    </ds:KeyInfo>
  </saml:SubjectConfirmationData>
</saml:SubjectConfirmation>
```

Note that the key in the `<ds:X509SKI>` element is in fact an alternate representation of the public key bound to the certificate in the `<ds:X509Certificate>` element. A relying party can confirm the subject by the matching the presented X.509 data to either of these elements.

2.5 Holder-of-Key Subject Confirmation Processing Rules

The ~~presenter~~subject presents one or more holder-of-key SAML assertions and an X.509 certificate to the ~~service provider~~relying party. The ~~presenter~~subject MUST prove possession of the private key corresponding to the public key of the presented certificate.

Regardless of the protocol used, any assertions relied upon MUST be valid according to the processing rules specified in [SAML2Core]. In particular, the ~~service provider~~relying party MUST verify the signature on each assertion containing a holder-of-key `<saml:SubjectConfirmation>` element. Any assertion that is not valid, or whose subject confirmation requirements cannot be met, SHOULD be discarded and SHOULD NOT be used to establish a security context for the subject.

The ~~service provider~~relying party MUST confirm that the presented certificate matches the content of the `<ds:X509Data>` element as follows:

- If the `<ds:X509Data>` element contains a `<ds:X509Certificate>` element, the ~~service provider~~relying party MUST confirm that the DER-encoded certificate bound to the assertion matches (byte for byte) the presented X.509 certificate.
- If the `<ds:X509Data>` element contains a `<ds:X509SKI>` element, the ~~service provider~~relying party MUST confirm that the hash value bound to the assertion matches the SHA-1 hash of the public key bound to the presented X.509 certificate .
- If the `<ds:X509Data>` element contains a `<ds:X509SubjectName>` element, the ~~service provider~~relying party MUST confirm that the DN bound to the assertion matches the subject distinguished name (DN) bound to the presented X.509 certificate. If, however, the ~~service provider~~relying party does not trust the certificate issuer to issue such a DN, the subject is not confirmed and the ~~service provider~~relying party SHOULD disregard the enclosing assertion.
- If the `<ds:X509Data>` element contains a `<ds:X509IssuerSerial>` element, the ~~service provider~~relying party MUST confirm that the issuer DN and issuer serial number bound to the assertion match the issuer DN and the issuer serial number (resp.) bound to the presented X.509 certificate. If the ~~service provider~~relying party does not trust the issuer to issue X.509 certificates, the subject is not confirmed and the ~~service provider~~relying party SHOULD disregard the enclosing assertion.

In the case of a `<ds:X509Certificate>` element or a `<ds:X509SKI>` element, the matching is a relatively straightforward process. If the `<ds:X509Data>` element contains a `<ds:X509SubjectName>` element or a `<ds:X509IssuerSerial>` element, however, the ~~service provider~~relying party MUST trust the issuer of the certificate before the subject can be considered confirmed. If such a trust relationship between the ~~service provider~~relying party and certificate issuer does not exist, the ~~service provider~~relying party SHOULD disregard the enclosing assertion.

2.6 Security and Privacy Considerations

This profile assumes the ~~presenter~~subject possesses an X.509 public key certificate and corresponding private key. For those deployments that wish to avoid or do not require a public key infrastructure (PKI), this may seem unnecessarily restrictive. However, the use of X.509 certificates provides a number of advantages. First, if the ~~presenter~~subject is the SAML requester, the subject DN of the certificate can be used in lieu of an `entityID`. Second, observe that the SSL/TLS protocol [RFC4346] requires the use of X.509 certificates. Finally, and most importantly, since there is no presumption of an underlying trust model for X.509 certificates, the full range of possible content for the `<ds:KeyInfo>` element is avoided. Those deployments that are in fact based on such a trust model, or wish to avoid X.509 certificates altogether, may choose to profile additional child elements such as `<ds:KeyName>` or `<ds:KeyValue>`.

Deployments that rely on holder-of-key SAML assertions will no doubt impose their own requirements on the X.509 certificates used to obtain those assertions. For example, some applications will require the certificate to be an X.509 end-entity certificate [RFC5280] issued by a trusted X.509 certification authority (CA) or a certificate based on a trusted X.509 end-entity certificate (such as an X.509 proxy certificate [RFC3820]). This specification imposes no such restrictions, however.

In particular, note that self-signed certificates are permitted with this specification. However, self-signed certificates should be used with care since it is well known that the use of such certificates may break certain implementations or protocols. For maximum interoperability, implementers are encouraged to use X.509 end-entity certificates [RFC5280] exclusively. For those deployments that wish to avoid or do not require a PKI, yet want to maintain interoperability, observe that so-called "meaningless X.509 certificates" [AIXCM] satisfy the requirements of X.509 end-entity certificates without belaboring the assumption of an underlying trust model.

Appendix A. Acknowledgments

The editors would like to acknowledge the contributions of the OASIS Security Services Technical Committee, whose voting members at the time of publication were:

- TBD

The editor would also like to acknowledge the following contributors:

- Joana M. F. da Trindade, Universidade Federal do Rio Grande do Sul (Brazil)

Appendix B. Revision History

Document ID	Date	Committer	Comment
sstc-saml2-holder-of-key-draft-01	7 Aug 2008	T. Scavo	Initial draft.
sstc-saml2-holder-of-key-draft-02	14 Aug 2008	T. Scavo	Remove all refs to `samlp:`
~~Document ID~~	~~Date~~	~~Committer~~	~~Comment~~
~~sstc-saml2-holder-of-key-draft-01~~	~~7 Aug 2008~~	~~T. Scavo~~	~~Initial draft.~~