



# SAML V2.0 Holder-of-Key Assertion Profile

## Working Draft 03, 7 September 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:

The *SAML V2.0 Holder-of-Key Assertion Profile* describes the issuing and processing of holder-of-key SAML assertions. Specifically, we show how a SAML issuer binds X.509 data to a `<ds:KeyInfo>` element and how a relying party confirms that a `<ds:KeyInfo>` element matches given X.509 data. The binding material used by the SAML issuer and the matching data used by the relying party are 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>.

## 34 Notices

35 Copyright © OASIS Open 2008. All Rights Reserved.

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

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

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

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

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

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

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

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

78 **Table of Contents**

79 1 Introduction.....4  
80 1.1 Notation.....4  
81 1.2 Normative References.....4  
82 1.3 Non-normative References.....5  
83 1.4 Conformance.....5  
84 1.4.1 SAML V2.0 Holder-of-Key Assertion Profile.....5  
85 2 SAML V2.0 Holder-of-Key Assertion Profile.....6  
86 2.1 Required Information.....6  
87 2.2 Profile Description.....6  
88 2.3 X.509 Certificate Usage.....6  
89 2.4 Issuing Holder-of-Key Assertions.....7  
90 2.4.1 Example.....7  
91 2.5 Processing Holder-of-Key Assertions.....8  
92 2.6 Security and Privacy Considerations.....9  
93 Appendix A. Acknowledgments.....10  
94 Appendix B. Revision History.....11  
95

# 1 Introduction

The *SAML V2.0 Holder-of-Key Assertion Profile* describes the issuing and processing of a holder-of-key SAML assertion, that is, an assertion containing a `<saml:SubjectConfirmation>` element whose `Method` attribute is set to `urn:oasis:names:tc:SAML:2.0:cm:holder-of-key`. Specifically, we describe the structural characteristics of a `<ds:KeyInfo>` element with bound X.509 data and show how a relying party confirms that such a `<ds:KeyInfo>` element matches given X.509 data. The binding material used by the SAML issuer and the matching data used by the relying party are obtained from a standard X.509 public key certificate.

## 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].

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>
- [RFC4514] K. Zeilenga. *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*. IETF RFC 4514, June 2006. <http://www.ietf.org/rfc/rfc4514.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

133 Standard, March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml->  
134 [profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)  
135 **[XMLSig]** D. Eastlake, J. Reagle, D. Solo, F. Hirsch, T. Roessler. *XML Signature Syntax*  
136 *and Processing (Second Edition)*. World Wide Web Consortium  
137 Recommendation, 10 June 2008. <http://www.w3.org/TR/xmlsig-core/>

## 138 1.3 Non-normative References

139 **[AIXCM]** T. Moreau. *Auto Issued X.509 Certificate Mechanism (AIXCM)*. IETF Internet-  
140 Draft, 6 August 2008. See [http://www.ietf.org/internet-drafts/draft-moreau-pkix-](http://www.ietf.org/internet-drafts/draft-moreau-pkix-aixcm-00.txt)  
141 [aixcm-00.txt](http://www.ietf.org/internet-drafts/draft-moreau-pkix-aixcm-00.txt)  
142 **[RFC3820]** S. Tuecke, V. Welch, D. Engert, L. Pearlman, M. Thompson. *Internet X.509*  
143 *Public Key Infrastructure (PKI) Proxy Certificate Profile*. IETF RFC 3820, June  
144 2004. <http://www.ietf.org/rfc/rfc3820.txt>  
145 **[RFC4346]** T. Dierks, E. Rescorla. *The Transport Layer Security (TLS) Protocol*. IETF  
146 RFC 4346, April 2006. <http://www.ietf.org/rfc/rfc4346.txt>  
147 **[RFC5280]** D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. *Internet*  
148 *X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)*  
149 *Profile*. IETF RFC 5280, May 2008. <http://www.ietf.org/rfc/rfc5280.txt>

## 150 1.4 Conformance

### 151 1.4.1 SAML V2.0 Holder-of-Key Assertion Profile

152 Both the SAML issuer and the relying party MUST conform to section .

153 A SAML issuer MUST follow the issuing rules in section . In particular, a SAML issuer MUST produce  
154 `<ds:KeyInfo>` elements that conform to section 2.4. Likewise, a relying party MUST follow the  
155 processing rules in section .

156 To claim conformance to this specification, a SAML issuer implementation MUST support the  
157 `<ds:X509Certificate>` element specified in section 2.4. Support for the remaining child elements  
158 specified in section 2.4 is OPTIONAL for SAML issuers.

159 Likewise a conforming relying party implementation MUST support the `<ds:X509Certificate>`  
160 element specified in section . Support for the remaining child elements specified in section is OPTIONAL  
161 for relying parties.

## 2 SAML V2.0 Holder-of-Key Assertion Profile

### 2.1 Required Information

**Identification:** urn:oasis:names:tc:SAML:2.0:profiles:holder-of-key

**Contact information:** [security-services-comment@lists.oasis-open.org](mailto: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:** Extends the holder-of-key confirmation method described in section 3.1 of [SAML2Prof].

### 2.2 Profile Description

Suppose a SAML response issued by a SAML issuer 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 SAML issuer binds selected X.509 data from an X.509 public key certificate to the <saml:SubjectConfirmation> element of a holder-of-key assertion.

The complementary process involves a relying party that confirms that the X.509 data bound to the assertion matches the data in a given X.509 certificate. We assume that the relying party trusts the SAML issuer to issue holder-of-key assertions. The SAML issuer, on the other hand, may not even know the intended relying party, so there is no underlying assumption that the SAML issuer trusts the relying party.

It is assumed that both the SAML issuer and the relying party have access to an X.509 public key certificate that is known to be associated with the subject of the assertion. How the X.509 certificate is obtained, however, is completely out of scope.

### 2.3 X.509 Certificate Usage

There are no explicit requirements with respect to the X.509 certificate(s) available to the SAML issuer and the relying party. That said, this specification mandates that the X.509 data bound to the SAML assertion by the SAML issuer MUST be taken from an X.509 public key certificate. Likewise the X.509 data matched against the bound X.509 data by the relying party MUST also be taken from an X.509 public key certificate. The specific characteristics of these certificates, however, are wholly out of scope with respect to this specification. In particular, there is no expectation that either the SAML issuer or the relying party trusts the issuer of the certificate, and therefore all portions of the certificate, apart from the X.509 data specified in the following sections, are out of scope.

The only exception is the case where the <ds:X509Data> element specified in section 2.4 contains a <ds:X509SubjectName> element or a <ds:X509SerialIssuer> element. In these two cases, the relying party MUST trust the X.509 issuer in order to confirm the subject. This is discussed more fully in section below.

## 198 2.4 Issuing Holder-of-Key Assertions

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

202 Suppose a SAML issuer wishes to issue a response containing one or more holder-of-key assertions. As  
203 a prerequisite, the SAML issuer MUST have access to an X.509 public key certificate known to be  
204 associated with the subject. The SAML issuer binds some or all of the X.509 data in the certificate to the  
205 `<saml:SubjectConfirmation>` element of a SAML assertion. The expected content of a holder-of-  
206 key `<saml:SubjectConfirmation>` element is specified in the next section.

### 207 KeyInfo Usage

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

- 214 • The `<ds:X509Data>` element MAY contain a `<ds:X509Certificate>` element. If it does, the  
215 `<ds:X509Certificate>` element MUST contain a base64 encoding of a DER-encoded X.509  
216 certificate.
- 217 • The `<ds:X509Data>` element MAY contain a `<ds:X509SKI>` element. If it does, the  
218 `<ds:X509SKI>` element MUST contain a base64 encoding of the SHA-1 hash of the public key  
219 bound to an X.509 certificate.
- 220 • The `<ds:X509Data>` element MAY contain a `<ds:X509SubjectName>` element. If it does, the  
221 `<ds:X509SubjectName>` element MUST contain the subject distinguished name (DN) bound to  
222 an X.509 certificate.
- 223 • The `<ds:X509Data>` element MAY contain a `<ds:X509IssuerSerial>` element. If it does,  
224 the `<ds:X509IssuerSerial>` element MUST contain the issuer DN and the issuer serial  
225 number (as specified in [XMLSig]) bound to an X.509 certificate.

226 Use of the `<ds:X509Certificate>` element or the `<ds:X509IssuerSerial>` element is most  
227 restrictive since each implies that the exact same certificate is used by both the SAML issuer and the  
228 relying party. Use of the `<ds:X509SKI>` element or the `<ds:X509SubjectName>` element is less  
229 restrictive since each permits a different certificate to be used by the relying party provided the certificate  
230 contains the same key or DN (resp.) used by the SAML issuer.

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

235 Note that the format of the DN contained in the `<ds:X509SubjectName>` element or the  
236 `<ds:X509IssuerSerial>` element is specified in [XMLSig]. In accordance with that specification, it is  
237 RECOMMENDED that the DN conform to [RFC4514] in all cases.

### 238 2.4.1 Example

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

```
241 <saml:SubjectConfirmation  
242   Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
```

```

243 <saml:SubjectConfirmationData
244   xsi:type="saml:KeyInfoConfirmationDataType">
245   <ds:KeyInfo>
246     <ds:X509Data>
247       <ds:X509Certificate>
248 MIIDuDCCAqACQCQCJZK8wF0xVXjANBgkqhkiG9w0BAQQFADCBnTELMaKGA1UEBhMCQlIxExZARBgNV
249 BAgtTC1NvbWUtU3RhdGUxEjAQBGNVBAcTCVNvbWUtQ2l0eTESMBAGA1UEChMJR1NvYyAyMDA4MRIw
250 EAYDVQQLLEw1HU29DIDIwMDgxZzAVBgNVBAMTDkpvYW5hIFRyaW5kYWRLMSQwIqYJKoZIhvcNAQkC
251 FhVzb211LWFkZHZJlc3NAAG9zdC5vcmcwHhcNMDgwNjE2MTcyMTQzWhcNMDkwNjE2MTcyMTQzWjCB
252 nTELMaKGA1UEBhMCQlIxExZARBgNVBAgtTC1NvbWUtU3RhdGUxEjAQBGNVBAcTCVNvbWUtQ2l0eTES
253 MBAGA1UEChMJR1NvYyAyMDA4MRIwEAYDVQQLLEw1HU29DIDIwMDgxZzAVBgNVBAMTDkpvYW5hIFRya
254 w5kYWRLMSQwIqYJKoZIhvcNAQkCBFhVzb211LWFkZHZJlc3NAAG9zdC5vcmcwgGEiMA0GCSqGSIB3
255 DQEBAAQUAA4IBDwAwggEKAoIBAQDIDVkdO2CCVYA0TspOPmcSNnivJq7jCacrgRPawKi3/pTuvnW
256 3c2XCpyT2s6Sks3Eg5T4HIXta5E+1OpN8VbTunVdSrac54r2uK8x+8AqX7M0wQw+98iGw9E2an5q
257 xRZfqgE1T5jWL/a/G1/e2TGlmp521W3k1nNtF8rYH39JpwBSZMeW7uHOSZOkT/pVvqPTgG7vUQT6
258 BiRh7PfwslrLomubbeQ6Z2m3Vnsv20E1FbPzswszh4X1gXj9bnyI2UsuoisW9Y4p4byjL3GJ/hxp
259 mjRjXs+aIpi0V3MH+jVJ98eomhlUFLaE83xycC8lns+FcCSQZ8RsbnaLZrtC8r7AgMBAAEwDQYJ
260 KoZIhvcNAQEEBQADggEBACwnWSEpwq5aE7QBdDNNXyok34RIonYi9690yw7i+JU7R/QdE42GERJS
261 DVKBN959ELLJf5d0vybGv08QWbZVQ7eBGn9xaZ7MhSnb1YNDXs9vuv1V2Dy32q1J5nCSzqpJDyln
262 lVfWe9UQMCJOO6ibUtWLhiDQ49kmMabgyYfX28qB6oRdVL+mDI/XtT+mkCgk4Rs78n4kbX6qnRlj
263 dE/YnibP1A7iMh8pQkv49J6sP9SeUmQ2zxKCT3tSRzzyWc8JjOZGuBYGQH19Xm7WEs4CXs7iZJW
264 E32frMatavMcTM/gnDtCc8tZAx12PSLOF1954vapfMjBhg3VTI6QRW//wPE=
265   </ds:X509Certificate>
266   <ds:X509SKI>YphoxnLNax/S0sdbdN3nD01wuR8=</ds:X509SKI>
267 </ds:X509Data>
268 </ds:KeyInfo>
269 </saml:SubjectConfirmationData>
270 </saml:SubjectConfirmation>

```

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

## 274 2.5 Processing Holder-of-Key Assertions

275 A relying party wishing to confirm the subject of a holder-of-key assertion MUST have access to an X.509  
276 public key certificate known to be associated with the subject. The relying party confirms the subject of  
277 the assertion by comparing the X.509 data in the certificate to the X.509 data bound to the assertion. If  
278 the X.509 data in the certificate matches the X.509 data bound to the assertion, the subject is said to be  
279 *confirmed*.

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

285 The relying party MUST confirm that the certificate matches the content of the `<ds:X509Data>` element  
286 as follows:

- 287 • If the `<ds:X509Data>` element contains a `<ds:X509Certificate>` element, the relying party  
288 MUST confirm that the DER-encoded certificate bound to the assertion matches the X.509  
289 certificate. Matching is done by comparing the certificates, or the hash values of the certificates,  
290 byte-for-byte.
- 291 • If the `<ds:X509Data>` element contains a `<ds:X509SKI>` element, the relying party MUST  
292 confirm that the hash value bound to the assertion matches the SHA-1 hash of the public key  
293 bound to the X.509 certificate .
- 294 • If the `<ds:X509Data>` element contains a `<ds:X509SubjectName>` element, the relying party  
295 MUST confirm that the subject distinguished name (DN) bound to the assertion matches the DN  
296 bound to the X.509 certificate. If, however, the relying party does not trust the certificate issuer to



297 issue such a DN, the subject is not confirmed and the relying party SHOULD disregard the  
298 enclosing assertion.

- 299 • If the `<ds:X509Data>` element contains a `<ds:X509IssuerSerial>` element, the relying party  
300 MUST confirm that the issuer DN and issuer serial number bound to the assertion match the  
301 issuer DN and the issuer serial number (resp.) bound to the X.509 certificate. If the relying party  
302 does not trust the certificate issuer to issue X.509 certificates, however, the subject is not  
303 confirmed and the relying party SHOULD disregard the enclosing assertion.

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

## 310 2.6 Security and Privacy Considerations

311 This profile assumes that both the SAML issuer and the relying party have access to an X.509 public key  
312 certificate. For those deployments that wish to avoid or do not require a public key infrastructure (PKI), this  
313 may seem unnecessarily restrictive. In fact, the use of X.509 certificates is typical and provides a number  
314 of advantages. First, if the subject is the SAML requester, the subject DN of the certificate may be used in  
315 lieu of an URI. Second, observe that the SSL/TLS protocol [RFC4346] requires the use of X.509  
316 certificates. Finally, and most importantly, since there is no presumption of an underlying trust model for  
317 X.509 certificates, the full range of possible content for the `<ds:KeyInfo>` element is avoided. Those  
318 deployments that are in fact based on such a trust model, or wish to avoid X.509 certificates altogether,  
319 may choose to profile additional child elements such as `<ds:KeyName>` or `<ds:KeyValue>`.

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

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

## 332 **Appendix A. Acknowledgments**

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

- 335 • TBD

336 The editor would also like to acknowledge the following contributors:

- 337 • 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 <code>samlp:</code>
sstc-saml2-holder-of-key-draft-03	7 Sep 2008	T. Scavo	Remove proof of possession requirement