



SAML V2.0 Information Card Token Profile

Working Draft 01, 19 August 2009

Specification URIs:

TBD

Technical Committee:

[OASIS Identity Metasystem Interoperability \(IMI\) TC](#)

Chair(s):

Marc Goodner, Microsoft Corporation

Anthony Nadalin, Microsoft Corporation

Editors:

Scott Cantor, Internet2

Abstract:

This profile describes a set of rules for identity providers and relying parties to follow when using SAML V2.0 assertions as managed information card security tokens, so that interoperability and security is achieved commensurate with other SAML authentication profiles.

Status

This document was last revised or approved by the IMI TC 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/imi>.

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/imi/ipr.php>).

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

29 Notices

30 Copyright © OASIS Open 2009. All Rights Reserved.

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

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

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

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

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

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

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

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

73 Table of Contents

74	1 Introduction.....	4
75	1.1 Notation.....	4
76	1.2 Normative References.....	5
77	1.3 Conformance.....	6
78	1.3.1 SAML V2.0 Information Card Token Profile.....	6
79	2 SAML V2.0 Information Card Token Profile.....	7
80	2.1 Required Information.....	7
81	2.2 Profile Overview.....	7
82	2.3 Identity Provider Requirements.....	7
83	2.3.1 Token Type.....	7
84	2.3.2 Identifying Token Issuers.....	7
85	2.3.3 General Assertion Requirements.....	8
86	2.3.4 Proof Keys and Subject Confirmation.....	8
87	2.3.5 Conditions.....	9
88	2.3.6 Encryption.....	9
89	2.4 Relying Party Requirements.....	9
90	2.4.1 Token Type.....	9
91	2.4.2 IdentifyingToken Issuers.....	9
92	2.4.3 Identifying Relying Parties.....	9
93	2.4.4 Identifying Claim Types.....	10
94	2.4.5 Assertion Validity.....	10
95	2.5 Use of SAML Metadata.....	10
96	2.6 Security Considerations.....	11
97	Appendix A. Acknowledgments.....	12
98	Appendix B. Revision History.....	13
99		

1 Introduction

OASIS has standardized a set of profiles for acquiring and delivering security tokens, collectively referred to as "Information Card" technology. These profiles are agnostic with respect to the format and semantics of a security token, but interoperability between issuing and relying parties cannot be achieved without additional rules governing the creation and use of the tokens exchanged. This document describes a set of rules for the use of SAML V2.0 assertions, as defined in [SAML2Core], as security tokens within the Information Card architecture.

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].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].
ic:	http://schemas.xmlsoap.org/ws/2005/05/identity	This is the Infocard namespace defined in the Identity Metasystem Interoperability standard SIP.
wsa:	http://www.w3.org/2005/08/addressing	This is the WS-Addressing namespace defined in the WS-Addressing specification [WS-Addr].
wsp:	http://schemas.xmlsoap.org/ws/2004/09/policy	This is the WS-Policy namespace defined in the March 2006 WS-Policy specification [WS-Policy].
sp:	http://schemas.xmlsoap.org/ws/2005/07/securitypolicy	This is the WS-SecurityPolicy namespace defined in the July 2005 WS-SecurityPolicy specification [WS-SecPol].
wst:	Either http://schemas.xmlsoap.org/ws/2005/02/trust/ or http://docs.oasis-open.org/ws-sx/ws-trust/200512	This is the WS-Trust namespace defined in the February 2005 WS-Trust specification [WS-Trust12] or the OASIS

Prefix	XML Namespace	Comments
		WS-Trust standard [WS-Trust13].
ds:	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace [XMLSig].
xsd:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.
xsi:	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].

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

125 1.2 Normative References

- 126 **[IMI]** M. Jones et al. *Identity Metasystem Interoperability V1.0*. OASIS Standard, July
127 2009. <http://docs.oasis-open.org/imi/identity/v1.0/os/identity-1.0-spec-os.pdf>.
- 128 **[RFC2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
129 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 130 **[SAML2Core]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
131 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID
132 saml-core-2.0-os. See [http://docs.oasis-open.org/security/saml/v2.0/saml-core-
133 2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf).
- 134 **[SAML2Meta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
135 (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-
136 os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 137 **[SAML2Prof]** J Hughes et al. *Profiles for the OASIS Security Assertion Markup Language
138 (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-profiles-2.0-os.
139 See <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.
- 140 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
141 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-
142 xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/). Note that this specification normatively references
143 [Schema2], listed below.
- 144 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide Web
145 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-
146 xmlschema-2-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/).
- 147 **[WS-Addr]** M. Gudgin et al. *WS-Addressing 1.0 Core*. World Wide Web Consortium
148 Recommendation, May 2006. See [http://www.w3.org/TR/2006/REC-ws-addr-
149 core-20060509/](http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/).
- 150 **[WS-Policy]** *Web Services Policy Framework, Version 1.2*. March 2006. See
151 <http://specs.xmlsoap.org/ws/2004/09/policy/ws-policy.pdf>.
- 152 **[WS-SecPol]** *Web Services Security Policy Language*. July 2005. See
153 <http://specs.xmlsoap.org/ws/2005/07/securitypolicy/ws-securitypolicy.pdf>.
- 154 **[WS-Trust12]** *Web Services Trust Language*. February 2005. See
155 <http://specs.xmlsoap.org/ws/2005/02/trust/WS-Trust.pdf>.
- 156 **[WS-Trust13]** *Web Services Trust Language*. OASIS Standard, March 2007. See
157 <http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf>.

158 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing, Second Edition*. World
159 Wide Web Consortium Recommendation, June 2008. See
160 <http://www.w3.org/TR/xmlsig-core/>.

161 **1.3 Conformance**

162 **1.3.1 SAML V2.0 Information Card Token Profile**

163 An identity provider implementation conforms to this profile if it can produce assertions consistent with the
164 normative text in section 2.3.

165 A relying party implementation conforms to this profile if it can accept assertions consistent with the
166 normative text of section 2.4.

167 Use of SAML V2.0 metadata [SAML2Meta] per section 2.5 is OPTIONAL.

2 SAML V2.0 Information Card Token Profile

2.1 Required Information

Identification: <http://docs.oasis-open.org/imi/ns/token/saml2/200908>

Contact information: imi-comment@lists.oasis-open.org

Description: Given below.

Updates: None.

2.2 Profile Overview

Identity providers and relying parties employing the Identity Metasystem Interoperability SIP profile to request and exchange security tokens are able to use arbitrary token formats, provided there is agreement on the token's syntax and semantics, and a way to connect the token's content to the supported protocol features.

This profile provides a set of requirements and guidelines for the use of SAML V2.0 assertions as security tokens that, where possible, emulates existing SAML V2.0 authentication profiles [SAML2Prof] so as to limit the amount of new work that must be done by existing software to support the use of Information Cards. It also provides for the use of SAML assertions in this new context that is safe and consistent with best practices in similar contexts.

This profile does not seek to alter the required behavior of existing identity selector software, or conflict with the profile defined by SIP.

2.3 Identity Provider Requirements

While the SAML V2.0 specification [SAML2Core] defines an identity provider solely in terms of the SAML Authentication Request protocol, the term is generally applicable to an entity that issues authentication assertions by means of other, similar protocols. In this case, the identity provider functions as an Identity Provider/Security Token Service (IP/STS) in the Information Card vocabulary, and issues assertions in response to `<wst:RequestSecurityToken>` messages [WS-Trust12] or [WS-Trust13].

As defined by SIP, the request contains information that provides input into the assertion creation process. The following sections outline requirements for interpreting this input and the resulting assertion content.

2.3.1 Token Type

The token type string used with SAML V2.0 assertions MUST be <http://docs.oasis-open.org/imi/ns/token/saml2/200908>.

This string appears in various content produced and consumed by an identity provider, such as (but not limited to) the `<wst:TokenType>` element.

2.3.2 Identifying Token Issuers

Information cards produced by identity providers MUST contain the identity provider's unique name as the value of the `<ic:Issuer>` element. This name corresponds to the SAML concept of an "entityID" and may correspond to an actual entityID in the SAML sense of the term, or a logically equivalent name for the identity provider.

204 **2.3.3 General Assertion Requirements**

205 Assertions issued in accordance with this profile MUST contain a single `<saml:AuthnStatement>` that
206 reflects the authentication of the token requester to the identity provider. It MAY contain a single
207 `<saml:AttributeStatement>` that carries one or more `<saml:Attribute>` elements reflecting the
208 claims requested by the relying party, in the manner specified by SIP.

209 When satisfying these requested claims, the resulting `<saml:Attribute>` element's `NameFormat` XML
210 attribute MUST be `urn:oasis:names:tc:SAML:2.0:attrname-format:uri` and its `Name` XML
211 attribute MUST correspond to the requested claim type's URI value (e.g., in `<ic:ClaimType>` elements).

212 A `<saml:NameID>` element MAY be included in the assertion's `<saml:Subject>` element. If the
213 requested claim types include a claim type with a URI corresponding to a SAML name identifier format
214 known to the identity provider, it may satisfy that claim request by including a `<saml:NameID>` element of
215 the proper format in the assertion's subject. If more than one claim type corresponding to a name identifier
216 format is requested, the identity provider MAY fault the request or choose any requested format, at its
217 discretion. If two such claim types are "required" by the relying party, a fault MUST be generated.

218 The assertion's `<saml:Subject>` element MUST contain at least one
219 `<saml:SubjectConfirmation>` element, the details of which are defined in section 2.3.4 below.

220 Finally, the assertion MUST be signed.

221 **2.3.4 Proof Keys and Subject Confirmation**

222 SIP defines three classes of "proof keys" that bind the issued token to key material controlled by the client:
223 symmetric, asymmetric, and no key. The notion of a proof key maps directly to a
224 `<saml:SubjectConfirmation>` element in the issued assertion.

225 If a token request does not include a `<wst:KeyType>` element, the identity provider SHOULD assume
226 that an asymmetric proof key is required.

227 Both symmetric and asymmetric proof key types generally correspond to the "holder-of-key" confirmation
228 method defined in section 3.1 of [SAML2Prof]. For the proof key types and algorithms specified by SIP,
229 the resulting assertion MUST contain a `<saml:SubjectConfirmation>` element with a `Method` of
230 `urn:oasis:names:tc:SAML:2.0:cm:holder-of-key`, as defined in that section. The
231 accompanying `<ds:KeyInfo>` element MUST identify the proof key. In the case of an RSA asymmetric
232 proof key, the key SHOULD be represented as a `<ds:RSAKeyValue>` element within a `<ds:KeyValue>`
233 element.

234 Proof key algorithms defined outside of SIP MAY specify alternate `<saml:SubjectConfirmation>`
235 content, if necessary.

236 The "no key" proof key type corresponds to the "bearer" confirmation method defined in section 3.3 of
237 [SAML2Prof]. The resulting assertion MUST contain a `<saml:SubjectConfirmation>` element with a
238 `Method` of `urn:oasis:names:tc:SAML:2.0:cm:bearer`, as defined in that section.

239 In the case of bearer assertions, the `<saml:SubjectConfirmation>` element MUST include a
240 `<saml:SubjectConfirmationData>` element containing a `NotOnOrAfter` XML attribute to limit their
241 use, typically to a very short window of time, although the exact duration may be use case dependent. The
242 attribute MAY be included for "holder-of-key" assertions, at the discretion of the identity provider.

243 The `<saml:SubjectConfirmationData>` element, if present, MUST NOT contain a `NotBefore` or
244 `Recipient` XML attribute. The `Address` XML attribute MAY be included to indicate the expected
245 network address of the client to the relying party.

246 Finally, note that other `<saml:SubjectConfirmation>` elements MAY be included at the discretion of
247 the identity provider.

248 **2.3.5 Conditions**

249 Assertions MAY contain a `<saml:Conditions>` element with `NotBefore` and `NotOnOrAfter`
250 attributes. This validity period can be independent of the window during which the client can present the
251 assertion to a relying party as a security token (see section 2.3.4), but of course must be a superset of that
252 window.

253 If the request contains a `<wsp:AppliesTo>` element, then a `<saml:AudienceRestriction>`
254 containing a `<saml:Audience>` element MUST be included with the value of that element.

255 Other conditions MAY be included at the discretion of the identity provider.

256 **2.3.6 Encryption**

257 If a suitable key belonging to the relying party is known, the identity provider SHOULD encrypt the
258 resulting assertion in accordance with section 6 of [SAML2Core], and return the result to the requester in
259 the form of a `<saml:EncryptedAssertion>` element.

260 If a public key belonging to the relying party is communicated to the identity provider in the
261 `<wst:RequestSecurityToken>` request message in the `<wsp:AppliesTo>` element, this key
262 SHOULD be used in preference to any other key known to the identity provider through other means
263 (e.g., SAML V2.0 metadata).

264 **2.4 Relying Party Requirements**

265 A relying party uses the mechanisms defined by SIP to request security tokens in the form of SAML2.0
266 assertions issued by particular or arbitrary identity providers. The following sections outline requirements
267 for describing a relying party's needs based on this profile.

268 **2.4.1 Token Type**

269 The token type string used with SAML V2.0 assertions MUST be `http://docs.oasis-`
270 `open.org/imi/ns/token/saml2/200908`.

271 This string appears in various content produced by a relying party, such as (but not limited to) the
272 `<wst:TokenType>` element.

273 **2.4.2 Identifying Token Issuers**

274 When identifying a requirement for a specific token issuer, the relying party SHOULD use the identity
275 provider's unique name (i.e., its "entityID").

276 **2.4.3 Identifying Relying Parties**

277 If the relying party provides security policy metadata (see section 3.1 of SIP), it MAY include a
278 `<wsp:AppliesTo>` element inside a `<sp:RequestSecurityTokenTemplate>` element that refers to
279 its own unique name (i.e., its "entityID") in the `<wsa:Address>` element.

280 If it does include a `<wsp:AppliesTo>` element, it SHOULD NOT identify itself using the location of its
281 endpoint, as this complicates the identity provider's ability to identify the relying party. A logical name
282 SHOULD be used instead.

283 2.4.4 Identifying Claim Types

284 SAML attributes required or desired by the relying party are identified by using the SAML attribute's `Name`
285 XML attribute in various places, such as the `<ic:ClaimType>` element's `Uri` XML attribute. Such SAML
286 attributes MUST have a `NameFormat` XML attribute of `urn:oasis:names:tc:SAML:2.0:attrname-`
287 `format:uri`.

288 A claim type URI corresponding to a SAML name identifier format MAY be used to request a particular
289 type of `<saml:NameID>` element in the resulting assertion. A relying party MUST NOT request more than
290 one "required" claim type corresponding to a name identifier format.

291 2.4.5 Assertion Validity

292 Relying parties SHOULD evaluate assertions using the rules defined by [SAML2Core] (and [SAML2Prof]
293 in the case of the defined subject confirmation methods). Invalid assertions SHOULD NOT be used to
294 authenticate clients that present them.

295 In assessing validity, a relying party MUST verify the signature over the assertion, evaluate any conditions
296 present, and successfully evaluate at least one `<saml:SubjectConfirmation>` element in the
297 assertion based on the presentation of the assertion. This may include verifying that the `NotOnOrAfter`
298 attribute in the `<saml:SubjectConfirmationData>` (if present) has not passed, subject to allowable
299 clock skew between it and the identity provider.

300 If the `<saml:SubjectConfirmationData>` includes an `Address` attribute, the relying party MAY
301 check the client address against it.

302 In the case of the "holder-of-key" method, the relying party MUST establish proof of possession by the
303 client of the key identified by the accompanying `<ds:KeyInfo>` element, such as through the use of a
304 message signature or authentication over a secure transport. The exact means are out of scope of this
305 profile.

306 In the case of the "bearer" method, the relying party MUST ensure that assertions are not replayed, by
307 maintaining the set of used `ID` values for the length of time for which the assertion would be considered
308 valid based on the `NotOnOrAfter` attribute in the `<saml:SubjectConfirmationData>` element.

309 2.5 Use of SAML Metadata

310 While not required, sites exchanging SAML assertions based on this profile MAY rely on SAML V2.0
311 metadata [SAML2Meta] as a way of deriving information about endpoints and keys, to supplement
312 mechanisms that exist within SIP. Where similarities or overlaps exist, precedence MUST be given to
313 metadata information exchanged using the mechanisms defined by SIP.

314 When referring to token issuers or relying parties by "logical" names, in the manner described by SIP, the
315 names used SHOULD correspond to the "entityID" values used in SAML metadata.

316 The value `http://docs.oasis-open.org/imi/ns/token/saml2/200908` MUST be used in the
317 `protocolSupportEnumeration` attribute to identify support for this profile within a
318 `<md:IDPSSODescriptor>` or `<md:SPSSODescriptor>` role.

319 If `<md:SingleSignOnService>` or `<md:AssertionConsumerService>` endpoints supporting this
320 profile are included, the same value MUST be used as the value of the `Binding` attribute. In addition, a
321 `<wsa:EndpointReference>` element MAY be included within an endpoint element to describe the
322 endpoint and its security policy in accordance with SIP.

323 2.6 Security Considerations

324 The Information Card model's support for hiding the identity of the relying party from the identity provider,
325 combined with constraints on the implementation of the model for use with web browsers, leads to
326 requests for "unconstrained" bearer assertions with no audience or subject confirmation conditions on
327 use. This is **extremely** dangerous and insecure, even if assertion validity is extremely short term. This
328 profile recommends against such a practice and urges implementations, if they do support such behavior,
329 to enable deployers to disable it by requiring requests for bearer assertions be accompanied by the
330 identity of the relying party.

331 Identity providers should generally make every attempt to encrypt the assertions they produce if a key for
332 the relying party can be established. If encryption is not used, then the identity provider should be aware of
333 the potential for exposure of the assertion's contents, both to the requester and potentially to network
334 observers if TLS/SSL is not used (particularly between the requester and the eventual relying party).

335 Caution, however, should be exercised in relying solely on the TLS/SSL certificate found at a relying
336 party's endpoint to identify the key. In particular, the key has to be authenticated in order to ensure that it
337 actually belongs to the eventual endpoint used by the client. Furthermore, there can be no guarantee that
338 the software responsible for decrypting the security token will have access to the corresponding private
339 key.

340 **Appendix A. Acknowledgments**

341 The editors would like to acknowledge the contributions of the OASIS Identity Metasystem Interoperability
342 Technical Committee, whose voting members at the time of publication were:

- 343 • TBD

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

- 345 • Jim Fox, University of Washington

346 **Appendix B. Revision History**

- 347 ● Draft 01, revised from Draft 02 of the SSTC-submitted version of this profile.