



SAML V2.0 Identity Assurance Profiles, Version 1.0

Committee Draft 01

22 September 2009

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.odt>
(Authoritative)

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.pdf>

Previous Version:

N/A

Latest Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.odt> (Authoritative)

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf>

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, Oracle Corporation

Thomas Hardjono, MIT Kerberos Consortium

Editor(s):

RL "Bob" Morgan, Internet2

Paul Madsen, NTT

Scott Cantor, Internet2

Related Work:

This specification profiles the SAML 2.0 Authentication Context [SAMLAC] mechanisms to allow SAML authentication requests and assertions to carry assurance information. It relies on the features specified in [SAMLMA] to represent information about a SAML entity as a SAML attribute associated with a metadata entry.

Declared XML Namespace(s):

N/A

34 **Abstract:**

35 This document specifies methods of representing assurance information as used in two
36 aspects of SAML. It profiles the use of SAML's Authentication Context mechanisms to express
37 per-authentication assurance information via authentication requests and assertions. Level-of-
38 Assurance (LOA) definitions in Identity Assurance Frameworks are expressed as a set of
39 authentication context classes. The document also specifies a means for representing
40 assurance certification status of entities in SAML metadata.

41 **Status:**

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

45 TC members should send comments on this specification to the TC's email list.

46 Others should send comments to the TC by using the "Send A Comment" button on
47 the TC's web page at <http://www.oasis-open.org/committees/security>.

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

51 The non-normative errata page for this specification is located at [http://www.oasis-](http://www.oasis-open.org/committees/security)
52 [open.org/committees/security](http://www.oasis-open.org/committees/security).

Notices

53

54 Copyright © OASIS® 2009. All Rights Reserved.

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

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

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

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

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

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

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

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

Table of Contents

98	1 Introduction.....	5
99	1.1 Motivation [Non-Normative].....	5
100	1.2 Limitations [Non-Normative].....	5
101	1.3 Terminology.....	6
102	1.4 Normative References.....	6
103	1.5 Non-normative References.....	7
104	2 AuthnContext Level-of-Assurance Profile.....	8
105	2.1 Required Information.....	8
106	2.2 AuthnContext Schema.....	8
107	2.3 Example LOA Framework classes.....	9
108	3 Identity Assurance Certification Attribute Profile.....	11
109	3.1 Required Information.....	11
110	3.2 Profile Overview.....	11
111	3.3 SAML Attribute Naming.....	11
112	3.4 Profile-Specific XML Attributes.....	11
113	3.5 SAML Attribute Values.....	11
114	3.6 Example.....	12
115	4 Conformance.....	13
116	4.1 AuthnContext Level-of-Assurance Profile Conformance.....	13
117	4.2 Identity Assurance Certification Attribute Profile Conformance.....	13
118	Appendix A.Acknowledgments.....	14
119	Appendix B.Revision History.....	15

1 Introduction

120

121 *Expressing Identity Assurance in SAML 2.0* provides standard means for parties using SAML to
122 exchange information regarding identity assurance. It defines, as a profile of the SAML Authentication
123 Context [SAMLAC] specification, a restricted version of the AuthnContext schema for representing
124 assurance indicators (sometimes called levels of assurance) defined by external documentation of any
125 given assurance framework. In addition, it defines a SAML attribute profile that may be used to
126 represent the certification status of an issuer of authentication statements (i.e., an Identity Provider)
127 regarding its conformance with the requirements of an identity assurance framework.

1.1 Motivation [Non-Normative]

128

129 Many organizations using federated service access have found it useful to define or adopt “identity
130 assurance frameworks,” such as [LibertyIAF]. Such frameworks offer a model for categorizing the
131 large number of possible combinations of registration processes, security mechanisms, and
132 authentication methods that underlie authentication processes into a smaller, more manageable set.
133 The term “levels of assurance” (LOA) is often used to refer to this concept, or a particular such set
134 (“assurance profiles” is also used). Different combinations of processes and technology are rated
135 according to the quality of assurance they can provide. Typically, a framework defines 3-5 levels or
136 profiles, ranging from low to high assurance. Relying parties then decide which LOA is required to
137 access specific protected resources, based on an assessment of the risk associated with those
138 resources – high risk requires high assurance, for example – and work with identity providers to ensure
139 that the requirements of that level are met.

140 Given this interest, it is useful for parties using SAML for federation to express in SAML authentication
141 messages the LOA requested by a relying party, and the LOA that is applicable to an authentication
142 response. The SAML authentication context specification [SAMLAC] defines a variety of options for
143 representing the details of identity management processes and mechanisms. The LOA profile in this
144 document is motivated by two related considerations:

- 145 • The SAML authentication context scheme is comprehensive, but quite complex. Deployers find
146 that this complexity is a barrier to designing authentication contexts that match their LOA
147 requirements.
- 148 • Representing the details of a LOA definition using the full expressiveness of the authentication
149 context schema results in XML documents that must be passed in-band with authentication
150 events and parsed by SAML implementations. In most cases, the processing requirements are
151 not sustainable and interoperability issues have not been explored.

152 The approach taken here simply represents each LOA in an assurance framework as a separate
153 authentication context class. Each LOA class is characterized by a URI, and the body of the schema
154 simply contains a reference to the external documentation that defines the LOA. These URI values are
155 conveyed in the `<RequestedAuthnContext>` element of an authentication request and the
156 `<AuthnContextClassRef>` element in the assertion within any authentication response.

157 Another common element in assurance programs is certification. See section 5.2 for background and
158 motivation for expressing assurance certification status in a standard fashion in SAML.

1.2 Limitations [Non-Normative]

159

160 A limitation to the LOA profile defined in this document is that the URIs representing the levels must be
161 configured into every system in the deployment, and the ordering of the URI levels must be decided
162 and configured out-of-band.

163 **1.3 Terminology**

164 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
165 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
166 described in IETF [RFC 2119]:

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

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

172 Listings of XML schemas appear like this.

173 Example code listings appear like this.

174
175 Conventional XML namespace prefixes are used throughout the listings in this specification to stand
176 for their respective namespaces as follows, whether or not a namespace declaration is present in the
177 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 [SAMLCore].
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 [SAMLCore].
xs:	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.

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

180 **1.4 Normative References**

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

183 **[SAMLAC]** OASIS Standard, *Authentication Context for the OASIS Security Assertion
184 Markup Language (SAML) V2.0*, March 2005. [http://docs.oasis-
185 open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf)

186 **[SAMLCore]** OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion
187 Markup Language (SAML) V2.0*, March 2005. [http://docs.oasis-
188 open.org/security/saml/v2.0/saml-core-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

189 **[SAMLMA]** OASIS Committee Specification, *SAML V2.0 Metadata Extension for Entity
190 Attributes*. August 2009. [http://docs.oasis-open.org/security/saml/Post2.0/ssstc-
191 metadata-attrib-cs-01.odt](http://docs.oasis-open.org/security/saml/Post2.0/ssstc-metadata-attrib-cs-01.odt)

192 **[SAMLMeta]** OASIS Standard, *Metadata for the OASIS Security Assertion Markup Language
193 (SAML) V2.0*, March 2005. [http://docs.oasis-open.org/security/saml/v2.0/saml-
194 metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

195 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
196 Consortium Recommendation, May 2001. See <http://www.w3.org/TR/2001/REC->

197 [xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/). Note that this specification normatively references
198 [Schema2], listed below.
199 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide
200 Web Consortium Recommendation, May 2001. See
201 <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>.

202 **1.5 Non-normative References**

203 **[LibertyIAF]** Russ Cutler, ed. Liberty Identity Assurance Framework 1.0, Liberty Alliance
204 Project, 2008.

2 AuthnContext Level-of-Assurance Profile

205

2.1 Required Information

206

207 **Identification:** urn:oasis:names:tc:SAML:2.0:ac:profiles:assurance

208 **Contact Information:** security-services-comment@lists.oasis-open.org

209 **Description:** Given below.

210 **Updates:** None.

2.2 AuthnContext Schema

211

212 The following schema redefines the basic abstract `AuthnContextDeclarationBaseType` to limit the
213 allowed elements to the `GoverningAgreements` element. It will be through this element that the
214 appropriate external assurance framework documentation will be referenced.

```
215 <?xml version="1.0" encoding="UTF-8"?>
216 <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
217   finalDefault="extension"
218   blockDefault="substitution" version="2.0">
219   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
220     <xs:annotation>
221       <xs:documentation>
222         Base class for building level-of-assurance style AuthnContext
223         class definitions.
224       </xs:documentation>
225     </xs:annotation>
226
227     <xs:complexType name="AuthnContextDeclarationBaseType">
228       <xs:complexContent>
229         <xs:restriction base="AuthnContextDeclarationBaseType">
230           <xs:sequence>
231             <xs:element ref="Identification"
232               minOccurs="0" maxOccurs="0"/>
233             <xs:element ref="TechnicalProtection"
234               minOccurs="0" maxOccurs="0"/>
235             <xs:element ref="OperationalProtection"
236               minOccurs="0" maxOccurs="0"/>
237             <xs:element ref="AuthnMethod"
238               minOccurs="0" maxOccurs="0"/>
239             <xs:element ref="GoverningAgreements"
240               minOccurs="1" maxOccurs="1"/>
241             <xs:element ref="Extension" minOccurs="0"
242               maxOccurs="unbounded"/>
243           </xs:sequence>
244           <xs:attribute name="ID" type="xs:ID" use="optional"/>
245         </xs:restriction>
246       </xs:complexContent>
247     </xs:complexType>
248
249     <xs:complexType name="GoverningAgreementRefType">
250       <xs:annotation>
251         <xs:documentation>
252           A specific restriction of this type specifying or
253           enumerating the governing document(s) and/or section
254           within such document(s) that define this particular
255           level of assurance.
```



```

256         </xs:documentation>
257     </xs:annotation>
258     <xs:complexContent>
259         <xs:restriction base="GoverningAgreementRefType">
260             <xs:attribute name="governingAgreementRef"
261                 type="xs:anyURI" use="required"/>
262         </xs:restriction>
263     </xs:complexContent>
264 </xs:complexType>
265 </xs:redefine>
266 </xs:schema>

```

267 The functional definition of the `GoverningAgreementRefType` is not changed from the original
268 schema in [SAMLAC], but documentation is added to serve as a reminder that definitions derived from
269 this schema should redefine `GoverningAgreementRefType` to suit a particular LOA purpose.

270 2.3 Example LOA Framework classes

271 We show here a set of LOA classes for a fictional FAF (Foo Assurance Framework) with three different
272 levels of assurance. The 3 LOA schemas will extend the base LOA schema defined above. Each LOA
273 schema will reference the corresponding section of the FAF documentation.

274 We define the following URIs to represent the 3 LOA

- 275 ● <http://foo.example.com/assurance/loa1>
- 276 ● <http://foo.example.com/assurance/loa2>
- 277 ● <http://foo.example.com/assurance/loa3>

278 As an example, the schema for the level 1 might look like:

```

279 <?xml version="1.0" encoding="UTF-8"?>
280 <xs:schema
281     targetNamespace="http://foo.example.com/assurance/loa1"
282     xmlns:xs="http://www.w3.org/2001/XMLSchema"
283     xmlns="http://foo.example.com/assurance/loa1"
284     finalDefault="extension"
285     blockDefault="substitution"
286     version="2.0">
287
288     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
289
290         <xs:annotation>
291             <xs:documentation>
292                 Class identifier:
293                 http://foo.example.com/assurance/loa1
294
295                 Defines Level 1 of FAF
296             </xs:documentation>
297         </xs:annotation>
298
299         <xs:complexType name="GoverningAgreementRefType">
300             <xs:complexContent>
301                 <xs:restriction base="GoverningAgreementRefType">
302                     <xs:attribute name="governingAgreementRef"
303                         type="xs:anyURI"
304                         fixed="http://foo.example.com/foo_assurance.pdf#sect
305                         ion1"
306                         use="required"/>

```

```
307         </xs:restriction>
308         </xs:complexContent>
309     </xs:complexType>
310 </xs:redefine>
311 </xs:schema>
```

312

313 The class schemas for the other 2 FAF LOA would refer to the corresponding section of the FAF
314 documentation.

3 Identity Assurance Certification Attribute Profile

A SAML attribute is defined to represent the certification status of an Identity Provider regarding its conformance to the elements of an identity assurance framework.

3.1 Required Information

Identification: urn:oasis:names:tc:SAML:2.0:attribute:profiles:assurance-certification

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

Description: Given below.

Updates: None.

3.2 Profile Overview

In some relatively simple scenarios where identity assurance is used, a relying party may have a direct business relationship with an organization operating an Identity Provider that satisfies the relying party that the practices of the Identity Provider conform to the requirements of an assurance framework. In a larger-scale scenario, a relying party may wish to rely on a third party (a “certification service”) to certify the practices of the Identity Provider organization. In this scenario, it is useful for the IdP’s certification status as determined by that certification service to be represented in a standard fashion, in a way that can be communicated securely among the various parties involved. The SAML metadata specification [SAMLMeta] defines means for information about SAML entities to be represented and communicated securely.

This profile defines a SAML attribute that can be applied to entries in a SAML metadata document to express certification status. To indicate that an Identity Provider (or group of Identity Providers) is certified as conformant with an LOA, the attribute defined in this profile is added to that identity Provider’s entity metadata as described in [SAMLMA]. This may be done using a `<saml:Attribute>` or a `<saml:Assertion>` element. A `<saml:Assertion>` element can be used to include an assurance certification attribute that is signed independently from the enclosing metadata.

3.3 SAML Attribute Naming

The `NameFormat` XML attribute in `<Attribute>` elements **MUST** be `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

This profile defines a single SAML attribute name:

`urn:oasis:names:tc:SAML:attribute:assurance-certification`

3.4 Profile-Specific XML Attributes

No additional XML attributes are defined for use with this attribute.

3.5 SAML Attribute Values

Values of this attribute are URIs representing LOAs as defined in section 2 of this document. Multiple values may be present. This document does not define any relationship between LOAs or define relying party behavior if multiple values are present. It is the responsibility of assurance framework documentation to specify whether, for example, certification at a “higher” LOA implies approval to assert a “lower” LOA.

352 3.6 Example

353 In this example a metadata publisher would place the SAML attribute statement in the IdP's entity
354 descriptor to indicate that the practices of the indicated IdP had been certified as conformant with the
355 requirements of the stated LOA. A party relying on this metadata could use this value as part of
356 determining whether and how to accept SAML authentication assertions from this IdP.

357

```
358 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"  
359   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  
360   xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"  
361   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  
362   entityID="https://IdentityProvider.example.com/SAML">  
363   <Extensions>  
364     <attr:EntityAttributes>  
365       <saml:Attribute  
366         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri"  
367         Name="urn:oasis:names:tc:SAML:attribute:assurance-  
368 certification">  
369         <saml:AttributeValue>  
370           http://foo.example.com/assurance/loa1  
371         </saml:AttributeValue>  
372       </saml:Attribute>  
373     </attr:EntityAttributes>  
374   </Extensions>  
375   <IDPSSODescriptor WantAuthnRequestsSigned="true"  
376     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  
377     <KeyDescriptor use="signing"> ... </KeyDescriptor>  
378     <NameIDFormat>...</NameIDFormat>  
379     <SingleSignOnService  
380       Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
381       Location="https://IdentityProvider.example.com/SAML/SSO/Browser"/>  
382     ...  
383   </IDPSSODescriptor>  
384   ...  
385 </EntityDescriptor>
```

386

387 **4 Conformance**

388 **4.1 AuthnContext Level-of-Assurance Profile Conformance**

389 To conform to this profile, implementations MUST support the use of the
390 `<samlp:RequestedAuthnContext>` and `<saml:AuthnContext>` elements defined by [SAMLCore].

391 **4.2 Identity Assurance Certification Attribute Profile Conformance**

392 An asserting party (typically, a metadata publisher) conforms to this profile if it can generate valid
393 SAML instances containing the SAML attribute defined in this profile.

394 A relying party (typically, a metadata consumer) conforms to this profile if it can process the SAML
395 attribute defined in this profile and make the results available for further processing.

396 All parties must also meet the conformance requirements in [SAMLMA].

397

Appendix A. Acknowledgments

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

- 400 • Rob Philpott, EMC Corporation
- 401 • Richard Franck, IBM
- 402 • John Bradley, Individual
- 403 • Scott Cantor, Internet2
- 404 • Nate Klingenstein, Internet2
- 405 • RL "Bob" Morgan, Internet2
- 406 • Thomas Hardjono, M.I.T.
- 407 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 408 • Frederick Hirsch, Nokia Corporation
- 409 • Paul Madsen, NTT Corporation
- 410 • Ari Kermaier, Oracle Corporation
- 411 • Hal Lockhart, Oracle Corporation
- 412 • Anil Saldhana, Red Hat
- 413 • Kent Spaulding, Skyworth TTG Holdings Limited
- 414 • Duane DeCouteau, Veterans Health Administration
- 415 • David Staggs, Veterans Health Administration

416

417

Appendix B. Revision History

- 418 ● Draft 01 – first draft of sstc-saml-loa-authncontext-profile
- 419 ● Draft 02 - minor tweaks to text. Removed editorial comments. Removed example class derived
420 from base class.
- 421 ● Draft 03 – removed the NIST 800 63 specific references and schema.
- 422 ● Draft 00 sstc-saml-assurance-profile : renamed to reflect added material. Added certification
423 motivation and specification.
- 424 ● Draft 01 sstc-saml-assurance-profile : added attribute profile conformance, added attribute
425 profile example, more description of certification usage, reorganized section numbering, put
426 conformance material in section 1.
- 427 ● Committee Draft, cosmetic edits.