



1

2 Authentication Context for the OASIS 3 Security Assertion Markup Language 4 (SAML) V2.0

5 **Committee Draft 04, 15 January 2005**

6 **Document identifier:**

7 sstc-saml-authn-context-2.0-cd-04

8 **Location:**

9 http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

10 **Editors:**

11 John Kemp, Nokia
12 Scott Cantor, Internet2
13 Prateek Mishra, Principal Identity
14 Rob Philpott, RSA Security
15 Eve Maler, Sun Microsystems

16 **SAML V2.0 Contributors:**

17 Conor P. Cahill, AOL
18 John Hughes, Atos Origin
19 Hal Lockhart, BEA Systems
20 Michael Beach, Boeing
21 Rebekah Metz, Booz Allen Hamilton
22 Rick Randall, Booz, Allen, Hamilton
23 Tim Alsop, CyberSafe Limited
24 Thomas Wisniewski, Entrust
25 Irving Reid, Hewlett-Packard
26 Paula Austel, IBM
27 Maryann Hondo, IBM
28 Michael McIntosh, IBM
29 Tony Nadalin, IBM
30 Nick Ragouzis, Individual
31 Scott Cantor, Internet2
32 RL 'Bob' Morgan, Internet2
33 Peter C Davis, Neustar
34 Jeff Hodges, Neustar
35 Frederick Hirsch, Nokia
36 John Kemp, Nokia
37 Paul Madsen, NTT
38 Charles Knouse, Oblix
39 Steve Anderson, OpenNetwork
40 Prateek Mishra, Principal Identity
41 John Linn, RSA Security
42 Rob Philpott, RSA Security
43 Jahan Moreh, Sigaba
44 Anne Anderson, Sun Microsystems

45 Gary Ellison, Sun Microsystems
46 Eve Maler, Sun Microsystems
47 Ron Monzillo, Sun Microsystems
48 Greg Whitehead, Trustgenix

49 **Abstract:**

50 This specification defines a syntax for the definition of authentication context declarations and an
51 initial list of authentication context classes for use with SAML.

52 **Status:**

53 This is a **Committee Draft** approved by the Security Services Technical Committee on 15
54 January 2005.

55 Committee members should submit comments and potential errata to the [security-](mailto:security-services@lists.oasis-open.org)
56 [services@lists.oasis-open.org](mailto:security-services@lists.oasis-open.org) list. Others should submit them by filling out the web form located
57 at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The
58 committee will publish on its web page (<http://www.oasis-open.org/committees/security>) a catalog
59 of any changes made to this document.

60 For information on whether any patents have been disclosed that may be essential to
61 implementing this specification, and any offers of patent licensing terms, please refer to the
62 Intellectual Property Rights web page for the Security Services TC ([http://www.oasis-](http://www.oasis-open.org/committees/security/ipr.php)
63 [open.org/committees/security/ipr.php](http://www.oasis-open.org/committees/security/ipr.php)).

64 Table of Contents

65	1 Introduction.....	4
66	1.1 Authentication Context Concepts.....	4
67	1.2 Notation and Terminology.....	4
68	2 Authentication Context Declaration.....	6
69	2.1 Data Model.....	6
70	2.2 Extensibility.....	7
71	2.3 Processing Rules.....	7
72	2.4 Schema.....	7
73	3 Authentication Context Classes.....	21
74	3.1 Advantages of Authentication Context Classes.....	21
75	3.2 Processing Rules.....	21
76	3.3 Extensibility.....	22
77	3.4 Schemas.....	22
78	3.4.1 Internet Protocol.....	22
79	3.4.2 InternetProtocolPassword.....	24
80	3.4.3 Kerberos.....	25
81	3.4.4 MobileOneFactorUnregistered.....	27
82	3.4.5 MobileTwoFactorUnregistered.....	30
83	3.4.6 MobileOneFactorContract.....	33
84	3.4.7 MobileTwoFactorContract.....	36
85	3.4.8 Password.....	39
86	3.4.9 PasswordProtectedTransport.....	41
87	3.4.10 PreviousSession.....	42
88	3.4.11 Public Key – X.509.....	44
89	3.4.12 Public Key – PGP.....	45
90	3.4.13 Public Key – SPKI.....	46
91	3.4.14 Public Key - XML Digital Signature.....	48
92	3.4.15 Smartcard.....	49
93	3.4.16 SmartcardPKI.....	51
94	3.4.17 SoftwarePKI.....	53
95	3.4.18 Telephony.....	55
96	3.4.19 Telephony ("Nomadic").....	56
97	3.4.20 Telephony (Personalized).....	58
98	3.4.21 Telephony (Authenticated).....	59
99	3.4.22 Secure Remote Password.....	60
100	3.4.23 SSL/TLS Certificate-Based Client Authentication.....	62
101	3.4.24 TimeSyncToken.....	64
102	3.4.25 Unspecified.....	65
103	4 References.....	66
104	Appendix A. Acknowledgments.....	68
105	Appendix B. Notices.....	70
106		

107 1 Introduction

108 This specification defines a syntax for the definition of authentication context declarations and an initial list
109 of authentication context classes.

110 1.1 Authentication Context Concepts

111 If a relying party is to rely on the authentication of a principal by an authentication authority, the relying
112 party may require information additional to the assertion itself in order to assess the level of confidence
113 they can place in that assertion. This specification defines an XML Schema for the creation of
114 Authentication Context declarations - XML documents that allow the authentication authority to provide to
115 the relying party this additional information. Additionally, this specification defines a number of
116 Authentication Context classes; categories into which many Authentication Context declarations will fall,
117 thereby simplifying their interpretation.

118 The OASIS Security Assertion Markup Language does not prescribe a single technology, protocol, or
119 policy for the processes by which authentication authorities issue identities to principals and by which
120 those principals subsequently authenticate themselves to the authentication authority. Different
121 authentication authorities will choose different technologies, follow different processes, and be bound by
122 different legal obligations with respect to how they authenticate principals.

123 The choices that an authentication authority makes here will be driven in large part by the requirements of
124 the relying parties with which the authentication authority interacts. These requirements themselves will be
125 determined by the nature of the service (that is, the sensitivity of any information exchanged, the
126 associated financial value, the relying parties' risk tolerance, etc.) that the relying party will be providing to
127 the principal.

128 Consequently, for anything other than trivial services, if the relying party is to place sufficient confidence in
129 the authentication assertions it receives from an authentication authority, it will be necessary for it to know
130 which technologies, protocols, and processes were used or followed for the original authentication
131 mechanism on which the authentication assertion is based. Armed with this information and trusting the
132 origin of the actual assertion, the relying party will be better able to make an informed entitlements
133 decision regarding what services the subject of the authentication assertion should be allowed to access.

134 *Authentication context* is defined as the information, additional to the authentication assertion itself, that
135 the relying party may require before it makes an entitlements decision with respect to an authentication
136 assertion. Such context may include, *but is not limited to*, the actual authentication method used (see the
137 SAML assertions and protocols specification [SAMLCore] for more information).

138 1.2 Notation and Terminology

139 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
140 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
141 described in IETF RFC 2119 [RFC 2119].

142 `Listings of XML schemas appear like this.`

143 `Example code listings appear like this.`

145 This specification uses schema documents conforming to W3C XML Schema [Schema1] and normative
146 text to describe the syntax and semantics of XML-encoded SAML assertions and protocol messages. In
147 cases of disagreement between the SAML authentication context schema documents and schema listings
148 in this specification, the schema documents take precedence. Note that in some cases the normative text
149 of this specification imposes constraints beyond those indicated by the schema documents.

150 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for

151 their respective namespaces as follows, whether or not a namespace declaration is present in the
152 example:

Prefix	XML Namespace	Comments
ac:	urn:oasis:names:tc:SAML:2.0:ac	This is the namespace defined in this specification and in a schema [SAMLAC-xsd].
xs:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1].

153

154 This specification uses the following typographical conventions in text: <SAML*Element*>,
155 <ns:ForeignElement>, XMLAttribute, **Datatype**, OtherKeyword.

156 2 Authentication Context Declaration

157 If a relying party is to rely on the authentication of another entity by an authentication authority, the relying
158 party may require information additional to the authentication itself to allow it to put the authentication into
159 a risk-management context. This information could include:

- 160 • The initial user identification mechanisms (for example, face-to-face, online, shared secret).
- 161 • The mechanisms for minimizing compromise of credentials (for example, credential renewal
162 frequency, client-side key generation).
- 163 • The mechanisms for storing and protecting credentials (for example, smartcard, password rules).
- 164 • The authentication mechanism or method (for example, password, certificate-based SSL).

165 The variations and permutations in the characteristics listed above guarantee that not all authentication
166 assertions will be the same with respect to the confidence that a relying party can place in it; a particular
167 authentication assertion will be characterized by the values for each of these (and other) variables.

168 A SAML authentication authority can deliver to a relying party the additional authentication context
169 information in the form of an authentication context declaration, an XML document either inserted directly
170 or referenced within the authentication assertion that the authentication authority provides to the relying
171 party.

172 SAML requesters are able to request that an authentication comply with a specified authentication context
173 by identifying that context in an authentication request. A requester may also specify that an authentication
174 must be conducted with an authentication context that *exceeds* some stated value (for some agreed
175 definition of "exceeds"). See the SAML assertions and protocols specification [SAMLCore] for more
176 information.

177 2.1 Data Model

178 A particular authentication context declaration defined in this specification will capture characteristics of
179 the processes, procedures, and mechanisms by which the authentication authority verified the subject
180 before issuing an identity, protects the secrets on which subsequent authentications are based, and the
181 mechanisms used for this authentication. These characteristics are categorized in the Authentication
182 Context schema as follows:

- 183 • Identification - Characteristics that describe the processes and mechanism the authentication
184 authority uses to initially create an association between a subject and the identity (or name) by which
185 the subject will be known.
- 186 • Technical Protection - Characteristics that describe how the "secret" (the knowledge or possession
187 of which allows the subject to authenticate to the authentication authority) is kept secure.
- 188 • Operational Protection - Characteristics that describe procedural security controls employed by the
189 authentication authority (for example, security audits, records archival).
- 190 • Authentication Method - Characteristics that define the mechanisms by which the subject of the
191 issued assertion authenticates to the authentication authority (for example, a password versus a
192 smartcard).
- 193 • Governing Agreements - Characteristics that describe the legal framework (e.g. liability constraints
194 and contractual obligations) underlying the authentication event and/or its associated technical
195 authentication infrastructure.

196 2.2 Extensibility

197 The authentication context declaration schema [SAMLAC-xsd] has well-defined extensibility points
198 through the <Extension> element. Authentication authorities can use this element to insert additional
199 authentication context details for the SAML assertions they issue (assuming that the consuming relying
200 party will be able to understand these extensions). These additional elements MUST be in a separate
201 XML Namespace to that of the authentication context declaration base or class schema that applies to the
202 declaration itself.

203 2.3 Processing Rules

204 Additional processing rules for authentication context declarations are specified in the SAML assertions
205 and protocols specification [SAMLCore]. Note that in most respects, these processing rules amount to
206 deployments sharing common interpretations of the relative strength or quality of particular authentication
207 context declarations and cannot be expressed in absolute terms or provided as rules that implementations
208 must follow.

209 2.4 Schema

210 This section lists the complete Authentication Context Types XML Schema [SAMLAC-Types], and the
211 Authentication Context XML schema [SAMLAC-xsd] itself, used for the validation of individual generalized
212 declarations. The types schema has no target namespace itself, and is then included by [SAMLAC-xsd].

```
213 <?xml version="1.0" encoding="UTF-8"?>
214 <xs:schema
215   xmlns:xs="http://www.w3.org/2001/XMLSchema"
216   elementFormDefault="qualified"
217   version="2.0">
218
219   <xs:annotation>
220     <xs:documentation>
221       Document identifier: sstc-saml-schema-authn-context-types-2.0
222       Location: http://www.oasis-
223 open.org/committees/documents.php?wg_abbrev=security
224       Revision history:
225         V2.0 CD-04 (January, 2005):
226         New core authentication context schema types for SAML V2.0.
227     </xs:documentation>
228   </xs:annotation>
229
230   <xs:element name="AuthenticationContextDeclaration"
231 type="AuthnContextDeclarationBaseType">
232     <xs:annotation>
233       <xs:documentation>
234         A particular assertion on an identity
235         provider's part with respect to the authentication
236         context associated with an authentication assertion.
237       </xs:documentation>
238     </xs:annotation>
239   </xs:element>
240
241   <xs:element name="Identification" type="IdentificationType">
242     <xs:annotation>
243       <xs:documentation>
244         Refers to those characteristics that describe the
245         processes and mechanisms
246         the Authentication Authority uses to initially create
247         an association between a Principal
248         and the identity (or name) by which the Principal will
249         be known
250       </xs:documentation>
251     </xs:annotation>
```

```

252 </xs:element>
253
254 <xs:element name="PhysicalVerification">
255   <xs:annotation>
256     <xs:documentation>
257       This element indicates that identification has been
258       performed in a physical
259       face-to-face meeting with the principal and not in an
260       online manner.
261     </xs:documentation>
262   </xs:annotation>
263   <xs:complexType>
264     <xs:attribute name="credentialLevel">
265       <xs:simpleType>
266         <xs:restriction base="xs:NMTOKEN">
267           <xs:enumeration value="primary"/>
268           <xs:enumeration value="secondary"/>
269         </xs:restriction>
270       </xs:simpleType>
271     </xs:attribute>
272   </xs:complexType>
273 </xs:element>
274
275 <xs:element name="WrittenConsent" type="ExtensionOnlyType"/>
276
277 <xs:element name="TechnicalProtection" type="TechnicalProtectionBaseType">
278   <xs:annotation>
279     <xs:documentation>
280       Refers to those characteristics that describe how the
281       'secret' (the knowledge or possession
282       of which allows the Principal to authenticate to the
283       Authentication Authority) is kept secure
284     </xs:documentation>
285   </xs:annotation>
286 </xs:element>
287
288 <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType">
289   <xs:annotation>
290     <xs:documentation>
291       This element indicates the types and strengths of
292       facilities
293       of a UA used to protect a shared secret key from
294       unauthorized access and/or use.
295     </xs:documentation>
296   </xs:annotation>
297 </xs:element>
298
299 <xs:element name="PrivateKeyProtection" type="PrivateKeyProtectionType">
300   <xs:annotation>
301     <xs:documentation>
302       This element indicates the types and strengths of
303       facilities
304       of a UA used to protect a private key from
305       unauthorized access and/or use.
306     </xs:documentation>
307   </xs:annotation>
308 </xs:element>
309
310 <xs:element name="KeyActivation" type="KeyActivationType">
311   <xs:annotation>
312     <xs:documentation>The actions that must be performed
313     before the private key can be used. </xs:documentation>
314   </xs:annotation>
315 </xs:element>
316
317 <xs:element name="KeySharing" type="KeySharingType">
318   <xs:annotation>

```



```

319     <xs:documentation>Whether or not the private key is shared
320         with the certificate authority.</xs:documentation>
321     </xs:annotation>
322 </xs:element>
323
324 <xs:element name="KeyStorage" type="KeyStorageType">
325     <xs:annotation>
326         <xs:documentation>
327             In which medium is the key stored.
328             memory - the key is stored in memory.
329             smartcard - the key is stored in a smartcard.
330             token - the key is stored in a hardware token.
331             MobileDevice - the key is stored in a mobile device.
332             MobileAuthCard - the key is stored in a mobile
333             authentication card.
334         </xs:documentation>
335     </xs:annotation>
336 </xs:element>
337
338 <xs:element name="SubscriberLineNumber" type="ExtensionOnlyType"/>
339 <xs:element name="UserSuffix" type="ExtensionOnlyType"/>
340
341 <xs:element name="Password" type="PasswordType">
342     <xs:annotation>
343         <xs:documentation>
344             This element indicates that a password (or passphrase)
345             has been used to
346             authenticate the Principal to a remote system.
347         </xs:documentation>
348     </xs:annotation>
349 </xs:element>
350
351 <xs:element name="ActivationPin" type="ActivationPinType">
352     <xs:annotation>
353         <xs:documentation>
354             This element indicates that a Pin (Personal
355             Identification Number) has been used to authenticate the Principal to
356             some local system in order to activate a key.
357         </xs:documentation>
358     </xs:annotation>
359 </xs:element>
360
361 <xs:element name="Token" type="TokenType">
362     <xs:annotation>
363         <xs:documentation>
364             This element indicates that a hardware or software
365             token is used
366             as a method of identifying the Principal.
367         </xs:documentation>
368     </xs:annotation>
369 </xs:element>
370
371 <xs:element name="TimeSyncToken" type="TimeSyncTokenType">
372     <xs:annotation>
373         <xs:documentation>
374             This element indicates that a time synchronization
375             token is used to identify the Principal. hardware -
376             the time synchronization
377             token has been implemented in hardware. software - the
378             time synchronization
379             token has been implemented in software. SeedLength -
380             the length, in bits, of the
381             random seed used in the time synchronization token.
382         </xs:documentation>
383     </xs:annotation>
384 </xs:element>
385

```

```

386 <xs:element name="Smartcard" type="ExtensionOnlyType">
387   <xs:annotation>
388     <xs:documentation>
389       This element indicates that a smartcard is used to
390       identity the Principal.
391     </xs:documentation>
392   </xs:annotation>
393 </xs:element>
394
395 <xs:element name="Length" type="LengthType">
396   <xs:annotation>
397     <xs:documentation>
398       This element indicates the minimum and/or maximum
399       ASCII length of the password which is enforced (by the UA or the
400       IdP). In other words, this is the minimum and/or maximum number of
401       ASCII characters required to represent a valid password.
402       min - the minimum number of ASCII characters required
403       in a valid password, as enforced by the UA or the IdP.
404       max - the maximum number of ASCII characters required
405       in a valid password, as enforced by the UA or the IdP.
406     </xs:documentation>
407   </xs:annotation>
408 </xs:element>
409
410 <xs:element name="ActivationLimit" type="ActivationLimitType">
411   <xs:annotation>
412     <xs:documentation>
413       This element indicates the length of time for which an
414       PIN-based authentication is valid.
415     </xs:documentation>
416   </xs:annotation>
417 </xs:element>
418
419 <xs:element name="Generation">
420   <xs:annotation>
421     <xs:documentation>
422       Indicates whether the password was chosen by the
423       Principal or auto-supplied by the Authentication Authority.
424       principalchosen - the Principal is allowed to choose
425       the value of the password. This is true even if
426       the initial password is chosen at random by the UA or
427       the IdP and the Principal is then free to change
428       the password.
429       automatic - the password is chosen by the UA or the
430       IdP to be cryptographically strong in some sense,
431       or to satisfy certain password rules, and that the
432       Principal is not free to change it or to choose a new password.
433     </xs:documentation>
434   </xs:annotation>
435
436   <xs:complexType>
437     <xs:attribute name="mechanism" use="required">
438       <xs:simpleType>
439         <xs:restriction base="xs:NMTOKEN">
440           <xs:enumeration value="principalchosen"/>
441           <xs:enumeration value="automatic"/>
442         </xs:restriction>
443       </xs:simpleType>
444     </xs:attribute>
445   </xs:complexType>
446 </xs:element>
447
448 <xs:element name="AuthnMethod" type="AuthnMethodBaseType">
449   <xs:annotation>
450     <xs:documentation>
451       Refers to those characteristics that define the
452       mechanisms by which the Principal authenticates to the Authentication

```

```

453     Authority.
454     </xs:documentation>
455     </xs:annotation>
456 </xs:element>
457
458 <xs:element name="PrincipalAuthenticationMechanism"
459 type="PrincipalAuthenticationMechanismType">
460   <xs:annotation>
461     <xs:documentation>
462       The method that a Principal employs to perform
463       authentication to local system components.
464     </xs:documentation>
465   </xs:annotation>
466 </xs:element>
467
468 <xs:element name="Authenticator" type="AuthenticatorBaseType">
469   <xs:annotation>
470     <xs:documentation>
471       The method applied to validate a principal's
472       authentication across a network
473     </xs:documentation>
474   </xs:annotation>
475 </xs:element>
476
477 <xs:element name="ComplexAuthenticator" type="ComplexAuthenticatorType">
478   <xs:annotation>
479     <xs:documentation>
480       Supports Authenticators with nested combinations of
481       additional complexity.
482     </xs:documentation>
483   </xs:annotation>
484 </xs:element>
485
486 <xs:element name="PreviousSession" type="ExtensionOnlyType">
487   <xs:annotation>
488     <xs:documentation>
489       Indicates that the Principal has been strongly
490       authenticated in a previous session during which the IdP has set a
491       cookie in the UA. During the present session the Principal has only
492       been authenticated by the UA returning the cookie to the IdP.
493     </xs:documentation>
494   </xs:annotation>
495 </xs:element>
496
497 <xs:element name="ResumeSession" type="ExtensionOnlyType">
498   <xs:annotation>
499     <xs:documentation>
500       Rather like PreviousSession but using stronger
501       security. A secret that was established in a previous session with
502       the Authentication Authority has been cached by the local system and
503       is now re-used (e.g. a Master Secret is used to derive new session
504       keys in TLS, SSL, WTLS).
505     </xs:documentation>
506   </xs:annotation>
507 </xs:element>
508
509 <xs:element name="ZeroKnowledge" type="ExtensionOnlyType">
510   <xs:annotation>
511     <xs:documentation>
512       This element indicates that the Principal has been
513       authenticated by a zero knowledge technique as specified in ISO/IEC
514       9798-5.
515     </xs:documentation>
516   </xs:annotation>
517 </xs:element>
518

```

```

519     <xs:element name="SharedSecretChallengeResponse"
520 type="SharedSecretChallengeResponseType"/>
521
522     <xs:complexType name="SharedSecretChallengeResponseType">
523       <xs:annotation>
524         <xs:documentation>
525           This element indicates that the Principal has been
526           authenticated by a challenge-response protocol utilizing shared secret
527           keys and symmetric cryptography.
528         </xs:documentation>
529       </xs:annotation>
530       <xs:sequence>
531         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
532       </xs:sequence>
533       <xs:attribute name="method" type="xs:anyURI" use="optional"/>
534     </xs:complexType>
535
536     <xs:element name="DigSig" type="PublicKeyType">
537       <xs:annotation>
538         <xs:documentation>
539           This element indicates that the Principal has been
540           authenticated by a mechanism which involves the Principal computing a
541           digital signature over at least challenge data provided by the IdP.
542         </xs:documentation>
543       </xs:annotation>
544     </xs:element>
545
546     <xs:element name="AsymmetricDecryption" type="PublicKeyType">
547       <xs:annotation>
548         <xs:documentation>
549           The local system has a private key but it is used
550           in decryption mode, rather than signature mode. For example, the
551           Authentication Authority generates a secret and encrypts it using the
552           local system's public key: the local system then proves it has
553           decrypted the secret.
554         </xs:documentation>
555       </xs:annotation>
556     </xs:element>
557
558     <xs:element name="AsymmetricKeyAgreement" type="PublicKeyType">
559       <xs:annotation>
560         <xs:documentation>
561           The local system has a private key and uses it for
562           shared secret key agreement with the Authentication Authority (e.g.
563           via Diffie Helman).
564         </xs:documentation>
565       </xs:annotation>
566     </xs:element>
567
568     <xs:complexType name="PublicKeyType">
569       <xs:sequence>
570         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
571       </xs:sequence>
572       <xs:attribute name="keyValidation" use="optional"/>
573     </xs:complexType>
574
575     <xs:element name="IPAddress" type="ExtensionOnlyType">
576       <xs:annotation>
577         <xs:documentation>
578           This element indicates that the Principal has been
579           authenticated through connection from a particular IP address.
580         </xs:documentation>
581       </xs:annotation>
582     </xs:element>
583
584     <xs:element name="SharedSecretDynamicPlaintext" type="ExtensionOnlyType">
585       <xs:annotation>

```

```

586     <xs:documentation>
587         The local system and Authentication Authority
588         share a secret key. The local system uses this to encrypt a
589         randomised string to pass to the Authentication Authority.
590     </xs:documentation>
591 </xs:annotation>
592 </xs:element>
593
594 <xs:element name="AuthenticatorTransportProtocol"
595 type="AuthenticatorTransportProtocolType">
596     <xs:annotation>
597         <xs:documentation>
598             The protocol across which Authenticator information is
599             transferred to an Authentication Authority verifier.
600         </xs:documentation>
601     </xs:annotation>
602 </xs:element>
603
604 <xs:element name="HTTP" type="ExtensionOnlyType">
605     <xs:annotation>
606         <xs:documentation>
607             This element indicates that the Authenticator has been
608             transmitted using bare HTTP utilizing no additional security
609             protocols.
610         </xs:documentation>
611     </xs:annotation>
612 </xs:element>
613
614 <xs:element name="IPSec" type="ExtensionOnlyType">
615     <xs:annotation>
616         <xs:documentation>
617             This element indicates that the Authenticator has been
618             transmitted using a transport mechanism protected by an IPSEC session.
619         </xs:documentation>
620     </xs:annotation>
621 </xs:element>
622
623 <xs:element name="WTLS" type="ExtensionOnlyType">
624     <xs:annotation>
625         <xs:documentation>
626             This element indicates that the Authenticator has been
627             transmitted using a transport mechanism protected by a WTLS session.
628         </xs:documentation>
629     </xs:annotation>
630 </xs:element>
631
632 <xs:element name="MobileNetworkNoEncryption" type="ExtensionOnlyType">
633     <xs:annotation>
634         <xs:documentation>
635             This element indicates that the Authenticator has been
636             transmitted solely across a mobile network using no additional
637             security mechanism.
638         </xs:documentation>
639     </xs:annotation>
640 </xs:element>
641
642 <xs:element name="MobileNetworkRadioEncryption" type="ExtensionOnlyType"/>
643 <xs:element name="MobileNetworkEndToEndEncryption" type="ExtensionOnlyType"/>
644
645 <xs:element name="SSL" type="ExtensionOnlyType">
646     <xs:annotation>
647         <xs:documentation>
648             This element indicates that the Authenticator has been
649             transmitted using a transport mechanism protected by an SSL or TLS
650             session.
651         </xs:documentation>
652     </xs:annotation>

```

```

653 </xs:element>
654
655 <xs:element name="PSTN" type="ExtensionOnlyType"/>
656 <xs:element name="ISDN" type="ExtensionOnlyType"/>
657 <xs:element name="ADSL" type="ExtensionOnlyType"/>
658
659 <xs:element name="OperationalProtection" type="OperationalProtectionType">
660   <xs:annotation>
661     <xs:documentation>
662       Refers to those characteristics that describe
663       procedural security controls employed by the Authentication Authority.
664     </xs:documentation>
665   </xs:annotation>
666 </xs:element>
667
668 <xs:element name="SecurityAudit" type="SecurityAuditType"/>
669 <xs:element name="SwitchAudit" type="ExtensionOnlyType"/>
670 <xs:element name="DeactivationCallCenter" type="ExtensionOnlyType"/>
671
672 <xs:element name="GoverningAgreements" type="GoverningAgreementsType">
673   <xs:annotation>
674     <xs:documentation>
675       Provides a mechanism for linking to external (likely
676       human readable) documents in which additional business agreements,
677       (e.g. liability constraints, obligations, etc) can be placed.
678     </xs:documentation>
679   </xs:annotation>
680 </xs:element>
681
682 <xs:element name="GoverningAgreementRef" type="GoverningAgreementRefType"/>
683
684 <xs:simpleType name="nymType">
685   <xs:restriction base="xs:NMTOKEN">
686     <xs:enumeration value="anonymity"/>
687     <xs:enumeration value="verinymity"/>
688     <xs:enumeration value="pseudonymity"/>
689   </xs:restriction>
690 </xs:simpleType>
691
692 <xs:complexType name="AuthnContextDeclarationBaseType">
693   <xs:sequence>
694     <xs:element ref="Identification" minOccurs="0"/>
695     <xs:element ref="TechnicalProtection" minOccurs="0"/>
696     <xs:element ref="OperationalProtection" minOccurs="0"/>
697     <xs:element ref="AuthnMethod" minOccurs="0"/>
698     <xs:element ref="GoverningAgreements" minOccurs="0"/>
699     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
700   </xs:sequence>
701   <xs:attribute name="ID" type="xs:ID" use="optional"/>
702 </xs:complexType>
703
704 <xs:complexType name="IdentificationType">
705   <xs:sequence>
706     <xs:element ref="PhysicalVerification" minOccurs="0"/>
707     <xs:element ref="WrittenConsent" minOccurs="0"/>
708     <xs:element ref="GoverningAgreements" minOccurs="0"/>
709     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
710   </xs:sequence>
711   <xs:attribute name="nym" type="nymType">
712     <xs:annotation>
713       <xs:documentation>
714         This attribute indicates whether or not the
715         Identification mechanisms allow the actions of the Principal to be
716         linked to an actual end user.
717       </xs:documentation>
718     </xs:annotation>
719   </xs:attribute>

```

```

720 </xs:complexType>
721
722 <xs:complexType name="TechnicalProtectionBaseType">
723   <xs:sequence>
724     <xs:choice minOccurs="0">
725       <xs:element ref="PrivateKeyProtection"/>
726       <xs:element ref="SecretKeyProtection"/>
727     </xs:choice>
728     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
729   </xs:sequence>
730 </xs:complexType>
731
732 <xs:complexType name="OperationalProtectionType">
733   <xs:sequence>
734     <xs:element ref="SecurityAudit" minOccurs="0"/>
735     <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
736     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
737   </xs:sequence>
738 </xs:complexType>
739
740 <xs:complexType name="AuthnMethodBaseType">
741   <xs:sequence>
742     <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
743     <xs:element ref="Authenticator" minOccurs="0"/>
744     <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
745     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
746   </xs:sequence>
747 </xs:complexType>
748
749 <xs:complexType name="GoverningAgreementsType">
750   <xs:sequence>
751     <xs:element ref="GoverningAgreementRef" maxOccurs="unbounded"/>
752   </xs:sequence>
753 </xs:complexType>
754
755 <xs:complexType name="GoverningAgreementRefType">
756   <xs:attribute name="governingAgreementRef" type="xs:anyURI" use="required"/>
757 </xs:complexType>
758
759 <xs:complexType name="PrincipalAuthenticationMechanismType">
760   <xs:sequence>
761     <xs:element ref="Password" minOccurs="0"/>
762     <xs:element ref="RestrictedPassword" minOccurs="0"/>
763     <xs:element ref="Token" minOccurs="0"/>
764     <xs:element ref="Smartcard" minOccurs="0"/>
765     <xs:element ref="ActivationPin" minOccurs="0"/>
766     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
767   </xs:sequence>
768   <xs:attribute name="preauth" type="xs:integer" use="optional"/>
769 </xs:complexType>
770
771 <xs:group name="AuthenticatorChoiceGroup">
772   <xs:choice>
773     <xs:element ref="PreviousSession"/>
774     <xs:element ref="ResumeSession"/>
775     <xs:element ref="DigSig"/>
776     <xs:element ref="Password"/>
777     <xs:element ref="RestrictedPassword"/>
778     <xs:element ref="ZeroKnowledge"/>
779     <xs:element ref="SharedSecretChallengeResponse"/>
780     <xs:element ref="SharedSecretDynamicPlaintext"/>
781     <xs:element ref="IPAddress"/>
782     <xs:element ref="AsymmetricDecryption"/>
783     <xs:element ref="AsymmetricKeyAgreement"/>
784     <xs:element ref="SubscriberLineNumber"/>
785     <xs:element ref="UserSuffix"/>
786     <xs:element ref="ComplexAuthenticator"/>

```

```

787     </xs:choice>
788 </xs:group>
789
790 <xs:group name="AuthenticatorSequenceGroup">
791   <xs:sequence>
792     <xs:element ref="PreviousSession" minOccurs="0"/>
793     <xs:element ref="ResumeSession" minOccurs="0"/>
794     <xs:element ref="DigSig" minOccurs="0"/>
795     <xs:element ref="Password" minOccurs="0"/>
796     <xs:element ref="RestrictedPassword" minOccurs="0"/>
797     <xs:element ref="ZeroKnowledge" minOccurs="0"/>
798     <xs:element ref="SharedSecretChallengeResponse" minOccurs="0"/>
799     <xs:element ref="SharedSecretDynamicPlaintext" minOccurs="0"/>
800     <xs:element ref="IPAddress" minOccurs="0"/>
801     <xs:element ref="AsymmetricDecryption" minOccurs="0"/>
802     <xs:element ref="AsymmetricKeyAgreement" minOccurs="0"/>
803     <xs:element ref="SubscriberLineNumber" minOccurs="0"/>
804     <xs:element ref="UserSuffix" minOccurs="0"/>
805     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
806   </xs:sequence>
807 </xs:group>
808
809 <xs:complexType name="AuthenticatorBaseType">
810   <xs:sequence>
811     <xs:group ref="AuthenticatorChoiceGroup"/>
812     <xs:group ref="AuthenticatorSequenceGroup"/>
813   </xs:sequence>
814 </xs:complexType>
815
816 <xs:complexType name="ComplexAuthenticatorType">
817   <xs:sequence>
818     <xs:group ref="AuthenticatorChoiceGroup"/>
819     <xs:group ref="AuthenticatorSequenceGroup"/>
820   </xs:sequence>
821 </xs:complexType>
822
823 <xs:complexType name="AuthenticatorTransportProtocolType">
824   <xs:sequence>
825     <xs:choice minOccurs="0">
826       <xs:element ref="HTTP"/>
827       <xs:element ref="SSL"/>
828       <xs:element ref="MobileNetworkNoEncryption"/>
829       <xs:element ref="MobileNetworkRadioEncryption"/>
830       <xs:element ref="MobileNetworkEndToEndEncryption"/>
831       <xs:element ref="WTLS"/>
832       <xs:element ref="IPSec"/>
833       <xs:element ref="PSTN"/>
834       <xs:element ref="ISDN"/>
835       <xs:element ref="ADSL"/>
836     </xs:choice>
837     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
838   </xs:sequence>
839 </xs:complexType>
840
841 <xs:complexType name="KeyActivationType">
842   <xs:sequence>
843     <xs:element ref="ActivationPin" minOccurs="0"/>
844     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
845   </xs:sequence>
846 </xs:complexType>
847
848 <xs:complexType name="KeySharingType">
849   <xs:attribute name="sharing" type="xs:boolean" use="required"/>
850 </xs:complexType>
851
852 <xs:complexType name="PrivateKeyProtectionType">
853   <xs:sequence>

```



```

854     <xs:element ref="KeyActivation" minOccurs="0"/>
855     <xs:element ref="KeyStorage" minOccurs="0"/>
856     <xs:element ref="KeySharing" minOccurs="0"/>
857     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
858   </xs:sequence>
859 </xs:complexType>
860
861 <xs:complexType name="PasswordType">
862   <xs:sequence>
863     <xs:element ref="Length" minOccurs="0"/>
864     <xs:element ref="Alphabet" minOccurs="0"/>
865     <xs:element ref="Generation" minOccurs="0"/>
866     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
867   </xs:sequence>
868   <xs:attribute name="ExternalVerification" type="xs:anyURI" use="optional"/>
869 </xs:complexType>
870
871 <xs:element name="RestrictedPassword" type="RestrictedPasswordType"/>
872
873 <xs:complexType name="RestrictedPasswordType">
874   <xs:complexContent>
875     <xs:restriction base="PasswordType">
876       <xs:sequence>
877         <xs:element name="Length" type="RestrictedLengthType" minOccurs="1"/>
878         <xs:element ref="Generation" minOccurs="0"/>
879         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
880       </xs:sequence>
881       <xs:attribute name="ExternalVerification" type="xs:anyURI"
882 use="optional"/>
883     </xs:restriction>
884   </xs:complexContent>
885 </xs:complexType>
886
887 <xs:complexType name="RestrictedLengthType">
888   <xs:complexContent>
889     <xs:restriction base="LengthType">
890       <xs:attribute name="min" use="required">
891         <xs:simpleType>
892           <xs:restriction base="xs:integer">
893             <xs:minInclusive value="3"/>
894           </xs:restriction>
895         </xs:simpleType>
896       </xs:attribute>
897       <xs:attribute name="max" type="xs:integer" use="optional"/>
898     </xs:restriction>
899   </xs:complexContent>
900 </xs:complexType>
901
902 <xs:complexType name="ActivationPinType">
903   <xs:sequence>
904     <xs:element ref="Length" minOccurs="0"/>
905     <xs:element ref="Alphabet" minOccurs="0"/>
906     <xs:element ref="Generation" minOccurs="0"/>
907     <xs:element ref="ActivationLimit" minOccurs="0"/>
908     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
909   </xs:sequence>
910 </xs:complexType>
911
912 <xs:element name="Alphabet" type="AlphabetType"/>
913 <xs:complexType name="AlphabetType">
914   <xs:attribute name="requiredChars" type="xs:string" use="required"/>
915   <xs:attribute name="excludedChars" type="xs:string" use="optional"/>
916   <xs:attribute name="case" type="xs:string" use="optional"/>
917 </xs:complexType>
918
919 <xs:complexType name="TokenType">
920   <xs:sequence>

```

```

921     <xs:element ref="TimeSyncToken"/>
922     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
923   </xs:sequence>
924 </xs:complexType>
925
926 <xs:simpleType name="DeviceTypeType">
927   <xs:restriction base="xs:NMTOKEN">
928     <xs:enumeration value="hardware"/>
929     <xs:enumeration value="software"/>
930   </xs:restriction>
931 </xs:simpleType>
932
933 <xs:simpleType name="booleanType">
934   <xs:restriction base="xs:NMTOKEN">
935     <xs:enumeration value="true"/>
936     <xs:enumeration value="false"/>
937   </xs:restriction>
938 </xs:simpleType>
939
940 <xs:complexType name="TimeSyncTokenType">
941   <xs:attribute name="DeviceType" type="DeviceTypeType" use="required"/>
942   <xs:attribute name="SeedLength" type="xs:integer" use="required"/>
943   <xs:attribute name="DeviceInHand" type="booleanType" use="required"/>
944 </xs:complexType>
945
946 <xs:complexType name="ActivationLimitType">
947   <xs:choice>
948     <xs:element ref="ActivationLimitDuration"/>
949     <xs:element ref="ActivationLimitUsages"/>
950     <xs:element ref="ActivationLimitSession"/>
951   </xs:choice>
952 </xs:complexType>
953
954 <xs:element name="ActivationLimitDuration" type="ActivationLimitDurationType">
955   <xs:annotation>
956     <xs:documentation>
957       This element indicates that the Key Activation Limit is
958       defined as a specific duration of time.
959     </xs:documentation>
960   </xs:annotation>
961 </xs:element>
962
963 <xs:element name="ActivationLimitUsages" type="ActivationLimitUsagesType">
964   <xs:annotation>
965     <xs:documentation>
966       This element indicates that the Key Activation Limit is
967       defined as a number of usages.
968     </xs:documentation>
969   </xs:annotation>
970 </xs:element>
971
972 <xs:element name="ActivationLimitSession" type="ActivationLimitSessionType">
973   <xs:annotation>
974     <xs:documentation>
975       This element indicates that the Key Activation Limit is
976       the session.
977     </xs:documentation>
978   </xs:annotation>
979 </xs:element>
980
981 <xs:complexType name="ActivationLimitDurationType">
982   <xs:attribute name="duration" type="xs:duration" use="required"/>
983 </xs:complexType>
984
985 <xs:complexType name="ActivationLimitUsagesType">
986   <xs:attribute name="number" type="xs:integer" use="required"/>
987 </xs:complexType>

```

```

988 <xs:complexType name="ActivationLimitSessionType"/>
989
990
991 <xs:complexType name="LengthType">
992   <xs:attribute name="min" type="xs:integer" use="required"/>
993   <xs:attribute name="max" type="xs:integer" use="optional"/>
994 </xs:complexType>
995
996 <xs:simpleType name="mediumType">
997   <xs:restriction base="xs:NMTOKEN">
998     <xs:enumeration value="memory"/>
999     <xs:enumeration value="smartcard"/>
1000    <xs:enumeration value="token"/>
1001    <xs:enumeration value="MobileDevice"/>
1002    <xs:enumeration value="MobileAuthCard"/>
1003   </xs:restriction>
1004 </xs:simpleType>
1005
1006 <xs:complexType name="KeyStorageType">
1007   <xs:attribute name="medium" type="mediumType" use="required"/>
1008 </xs:complexType>
1009
1010 <xs:complexType name="SecretKeyProtectionType">
1011   <xs:sequence>
1012     <xs:element ref="KeyActivation" minOccurs="0"/>
1013     <xs:element ref="KeyStorage" minOccurs="0"/>
1014     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1015   </xs:sequence>
1016 </xs:complexType>
1017
1018 <xs:complexType name="SecurityAuditType">
1019   <xs:sequence>
1020     <xs:element ref="SwitchAudit" minOccurs="0"/>
1021     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1022   </xs:sequence>
1023 </xs:complexType>
1024
1025 <xs:complexType name="ExtensionOnlyType">
1026   <xs:sequence>
1027     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1028   </xs:sequence>
1029 </xs:complexType>
1030
1031 <xs:element name="Extension" type="ExtensionType"/>
1032
1033 <xs:complexType name="ExtensionType">
1034   <xs:sequence>
1035     <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
1036   </xs:sequence>
1037 </xs:complexType>
1038
1039 </xs:schema>
1040

```

1041

1042

```

1043 <?xml version="1.0" encoding="UTF-8"?>
1044 <xs:schema
1045   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
1046   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1047   xmlns="urn:oasis:names:tc:SAML:2.0:ac"
1048   blockDefault="substitution"
1049   version="2.0">
1050
1051   <xs:annotation>
1052     <xs:documentation>

```

```
1053     Document identifier: sstc-saml-schema-authn-context-2.0
1054     Location: http://www.oasis-
1055     open.org/committees/documents.php?wg_abbrev=security
1056     Revision history:
1057     V2.0 CD-04 (January, 2005):
1058     New core authentication context schema for SAML V2.0.
1059     This is just an include of all types from the schema
1060     referred to in the include statement below.
1061     </xs:documentation>
1062 </xs:annotation>
1063
1064     <xs:include schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd"/>
1065
1066 </xs:schema>
```

1067 **3 Authentication Context Classes**

1068 The number of permutations of different characteristics ensures that there is a theoretically infinite number
1069 of unique authentication contexts. The implication is that, in theory, any particular relying party would be
1070 expected to be able to parse arbitrary authentication context declarations and, more importantly, to
1071 analyze the declaration in order to assess the “quality” of the associated authentication assertion. Making
1072 such an assessment is non-trivial.

1073 Fortunately, an optimization is possible. In practice many authentication contexts will fall into categories
1074 determined by industry practices and technology. For instance, many B2C web browser authentication
1075 contexts will be (partially) defined by the principal authenticating to the authentication authority through the
1076 presentation of a password over an SSL protected session. In the enterprise world, certificate-based
1077 authentication will be common. Of course, the full authentication context is not limited to the specifics of
1078 how the principal authenticated. Nevertheless, the authentication method is often the most visible
1079 characteristic and as such, can serve as a useful classifier for a class of related authentication contexts.

1080 The concept is expressed in this specification as a definition of a series of authentication context classes.
1081 Each class defines a proper subset of the full set of authentication contexts. Classes have been chosen
1082 as representative of the current practices and technologies for authentication technologies, and provide
1083 asserting and relying parties a convenient shorthand when referring to authentication context issues.

1084 For instance, an authentication authority may include with the complete authentication context declaration
1085 it provides to a relying party an assertion that the authentication context also belongs to an authentication
1086 context class. For some relying parties, this assertion is sufficient detail for it to be able to assign an
1087 appropriate level of confidence to the associated authentication assertion. Other relying parties might
1088 prefer to examine the complete authentication context declaration itself. Likewise, the ability to refer to an
1089 authentication context class rather than being required to list the complete details of a specific
1090 authentication context declaration will simplify how the relying party can express its desires and/or
1091 requirements to an authentication authority.

1092 **3.1 Advantages of Authentication Context Classes**

1093 The introduction of the additional layer of classes and the definition of an initial list of representative and
1094 flexible classes are expected to:

- 1095 • Make it easier for the authentication authority and relying party to come to an agreement on what are
1096 acceptable authentication contexts by giving them a framework for discussion.
- 1097 • Make it easier for relying parties to indicate their preferences when requesting a step-up
1098 authentication assertion from an authentication authority.
- 1099 • Simplify for relying parties the burden of processing authentication context declarations by giving
1100 them the option of being satisfied by the associated class.
- 1101 • Insulate relying parties from the impact of new authentication technologies.
- 1102 • Make it easier for authentication authorities to publish their authentication capabilities, for example,
1103 through WSDL.

1104 **3.2 Processing Rules**

1105 Further processing rules for authentication context classes are described in the SAML assertions and
1106 protocols specification [SAMLCore]. Note that in most respects, these processing rules amount to
1107 deployments sharing common interpretations of the relative strength or quality of particular authentication
1108 context classes and cannot be expressed in absolute terms or provided as rules that implementations
1109 must follow.

1110 3.3 Extensibility

1111 As does the core authentication context declaration schema, the separate authentication context class
1112 schemas allow the `<Extension>` element in certain locations of the tree structure. In general, where the
1113 `<Extension>` element occurred as a child of an `<xs:choice>` element, this option was removed in
1114 creating the appropriate class schema definition as a restriction of the base type. When the
1115 `<Extension>` element occurred as an optional child of an `<xs:sequence>` element, the `<Extension>`
1116 element was allowed to remain in addition to any required elements.

1117 Consequently, authentication context declarations can include the `<Extension>` element (with additional
1118 elements in different namespaces) and still conform to authentication context class schemas (if they meet
1119 the other requirements of the schema of course).

1120 The authentication context class schemas restrict type definitions in the base authentication context
1121 schema. As an extension point, the authentication context class schemas themselves can be further
1122 restricted – their type definitions serving as base types in some other schema (potentially defined by
1123 some community wishing a more tightly defined authentication context class). To prevent logical
1124 inconsistencies, any such schema extensions can only further constrain the type definitions of the class
1125 schema. To enforce this constraint, the authentication context class schemas are defined with the
1126 `finalDefault="extension"` attribute on the `<schema>` element to prevent this type of derivation.

1127 Additional authentication context classes MAY be developed by groups other than the Security Services
1128 Technical Committee. OASIS members may wish to document and submit them for consideration by the
1129 SSTC in a future version of the specification, and other groups may simply wish to inform the committee
1130 of their work. Please refer to the SSTC web site for further details.

1131 Guidelines for the specification of new context classes are as follows:

- 1132 • Specify a URI that uniquely identifies the context class.
- 1133 • Provide contact information for the author of the class.
- 1134 • Provide a textual description of the circumstances under which this class should be used.
- 1135 • Provide a valid XML schema [Schema1] document implementing the class.

1136 Authors of new classes are encouraged to review the classes defined within this specification in order to
1137 guide their work.

1138 3.4 Schemas

1139 Authentication context classes are listed in the following subsections. The classes are listed in
1140 alphabetical order; no other ranking is implied by the order of classes. Classes are uniquely identified by
1141 URIs with the following initial stem:

```
1142 urn:oasis:names:tc:SAML:2.0:ac:classes
```

1143 The class schemas are defined as restrictions of parts of the base authentication context "types" schema.
1144 XML instances that validate against a given authentication context class schema are said to *conform* to
1145 that authentication context class.

1146 Note that because the class schema imports and redefines the elements and types into the class schema
1147 namespace, a class-conforming authentication context declaration does not simultaneously validate
1148 against the base authentication context schema.

1149 3.4.1 Internet Protocol

1150 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol

1151 Note that this URI is also used as the target namespace in the corresponding authentication context class
1152 schema document ([SAMLAC-IP]).

1153 The Internet Protocol class is applicable when a principal is authenticated through the use of a provided IP
1154 address.

```
1155 <?xml version="1.0" encoding="UTF-8"?>
1156
1157 <xs:schema
1158   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1159   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1160   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1161   finalDefault="extension"
1162   blockDefault="substitution"
1163   version="2.0">
1164
1165   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
1166
1167     <xs:annotation>
1168       <xs:documentation>
1169         Class identifier:
1170 urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
1171         Document identifier: sstc-saml-schema-authn-context-ip-2.0
1172         Location: http://www.oasis-
1173 open.org/committees/documents.php?wg_abbrev=security
1174         Revision history:
1175           V2.0 CD-04 (January, 2005):
1176             New authentication context class schema for SAML V2.0.
1177       </xs:documentation>
1178     </xs:annotation>
1179
1180     <xs:complexType name="AuthnContextDeclarationBaseType">
1181       <xs:complexContent>
1182         <xs:restriction base="AuthnContextDeclarationBaseType">
1183           <xs:sequence>
1184             <xs:element ref="Identification" minOccurs="0"/>
1185             <xs:element ref="TechnicalProtection" minOccurs="0"/>
1186             <xs:element ref="OperationalProtection" minOccurs="0"/>
1187             <xs:element ref="AuthnMethod"/>
1188             <xs:element ref="GoverningAgreements" minOccurs="0"/>
1189             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1190           </xs:sequence>
1191           <xs:attribute name="ID" type="xs:ID" use="optional"/>
1192         </xs:restriction>
1193       </xs:complexContent>
1194     </xs:complexType>
1195
1196     <xs:complexType name="AuthnMethodBaseType">
1197       <xs:complexContent>
1198         <xs:restriction base="AuthnMethodBaseType">
1199           <xs:sequence>
1200             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1201             <xs:element ref="Authenticator"/>
1202             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1203             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1204           </xs:sequence>
1205         </xs:restriction>
1206       </xs:complexContent>
1207     </xs:complexType>
1208
1209     <xs:complexType name="AuthenticatorBaseType">
1210       <xs:complexContent>
1211         <xs:restriction base="AuthenticatorBaseType">
1212           <xs:sequence>
1213             <xs:element ref="IPAddress"/>
1214           </xs:sequence>
1215         </xs:restriction>
1216       </xs:complexContent>
1217     </xs:complexType>
1218
```

```
1219     </xs:redefine>
1220
1221 </xs:schema>
```

1222 3.4.2 InternetProtocolPassword

1223 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword

1224 Note that this URI is also used as the target namespace in the corresponding authentication context class
1225 schema document ([SAMLAC-IPP]).

1226 The Internet Protocol Password class is applicable when a principal is authenticated through the use of a
1227 provided IP address, in addition to a username/password.

```
1228 <?xml version="1.0" encoding="UTF-8"?>
1229
1230 <xs:schema
1231   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassw
1232   ord"
1233   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1234   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1235   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
1236   finalDefault="extension"
1237   blockDefault="substitution"
1238   version="2.0">
1239
1240   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
1241
1242     <xs:annotation>
1243       <xs:documentation>
1244         Class identifier:
1245         urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
1246         Document identifier: sstc-saml-schema-authn-context-ippword-2.0
1247         Location: http://www.oasis-
1248         open.org/committees/documents.php?wg_abbrev=security
1249         Revision history:
1250         V2.0 CD-04 (January, 2005):
1251         New authentication context class schema for SAML V2.0.
1252       </xs:documentation>
1253     </xs:annotation>
1254
1255     <xs:complexType name="AuthnContextDeclarationBaseType">
1256       <xs:complexContent>
1257         <xs:restriction base="AuthnContextDeclarationBaseType">
1258           <xs:sequence>
1259             <xs:element ref="Identification" minOccurs="0"/>
1260             <xs:element ref="TechnicalProtection" minOccurs="0"/>
1261             <xs:element ref="OperationalProtection" minOccurs="0"/>
1262             <xs:element ref="AuthnMethod"/>
1263             <xs:element ref="GoverningAgreements" minOccurs="0"/>
1264             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1265           </xs:sequence>
1266           <xs:attribute name="ID" type="xs:ID" use="optional"/>
1267         </xs:restriction>
1268       </xs:complexContent>
1269     </xs:complexType>
1270
1271     <xs:complexType name="AuthnMethodBaseType">
1272       <xs:complexContent>
1273         <xs:restriction base="AuthnMethodBaseType">
1274           <xs:sequence>
1275             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1276             <xs:element ref="Authenticator"/>
1277             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1278             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1279           </xs:sequence>
```



```

1280     </xs:restriction>
1281   </xs:complexContent>
1282 </xs:complexType>
1283
1284   <xs:complexType name="AuthenticatorBaseType">
1285     <xs:complexContent>
1286       <xs:restriction base="AuthenticatorBaseType">
1287         <xs:sequence>
1288           <xs:element ref="Password"/>
1289           <xs:element ref="IPAddress"/>
1290           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1291         </xs:sequence>
1292       </xs:restriction>
1293     </xs:complexContent>
1294   </xs:complexType>
1295
1296 </xs:redefine>
1297
1298 </xs:schema>

```

1299 3.4.3 Kerberos

1300 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

1301 Note that this URI is also used as the target namespace in the corresponding authentication context class
 1302 schema document ([SAMLAC-Kerb]).

1303 This class is applicable when the principal has authenticated using a password to a local authentication
 1304 authority, in order to acquire a Kerberos ticket. That Kerberos ticket is then used for subsequent network
 1305 authentication.

1306 **Note:** It is possible for the authentication authority to indicate (via this context class) a pre-
 1307 authentication data type which was used by the Kerberos Key Distribution Center [RFC 1510]
 1308 when authenticating the principal. The method used by the authentication authority to obtain this
 1309 information is outside of the scope of this specification, but it is strongly recommended that a
 1310 trusted method be deployed to pass the pre-authentication data type and any other Kerberos
 1311 related context details (e.g. ticket lifetime) to the authentication authority.

```

1312 <?xml version="1.0" encoding="UTF-8"?>
1313
1314 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1315   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1316   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1317   finalDefault="extension"
1318   blockDefault="substitution"
1319   version="2.0">
1320
1321   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
1322
1323     <xs:annotation>
1324       <xs:documentation>
1325         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
1326         Document identifier: sstc-saml-schema-authn-context-kerberos-2.0
1327         Location: http://www.oasis-
1328 open.org/committees/documents.php?wg_abbrev=security
1329         Revision history:
1330           V2.0 CD-04 (January, 2005):
1331             New authentication context class schema for SAML V2.0.
1332       </xs:documentation>
1333     </xs:annotation>
1334
1335     <xs:complexType name="AuthnContextDeclarationBaseType">
1336       <xs:complexContent>
1337         <xs:restriction base="AuthnContextDeclarationBaseType">
1338           <xs:sequence>

```

```

1339         <xs:element ref="Identification" minOccurs="0"/>
1340         <xs:element ref="TechnicalProtection" minOccurs="0"/>
1341         <xs:element ref="OperationalProtection" minOccurs="0"/>
1342         <xs:element ref="AuthnMethod"/>
1343         <xs:element ref="GoverningAgreements" minOccurs="0"/>
1344         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1345     </xs:sequence>
1346     <xs:attribute name="ID" type="xs:ID" use="optional"/>
1347 </xs:restriction>
1348 </xs:complexContent>
1349 </xs:complexType>
1350
1351 <xs:complexType name="AuthnMethodBaseType">
1352     <xs:complexContent>
1353         <xs:restriction base="AuthnMethodBaseType">
1354             <xs:sequence>
1355                 <xs:element ref="PrincipalAuthenticationMechanism"/>
1356                 <xs:element ref="Authenticator"/>
1357                 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1358                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1359             </xs:sequence>
1360         </xs:restriction>
1361     </xs:complexContent>
1362 </xs:complexType>
1363
1364 <xs:complexType name="PrincipalAuthenticationMechanismType">
1365     <xs:complexContent>
1366         <xs:restriction base="PrincipalAuthenticationMechanismType">
1367             <xs:sequence>
1368                 <xs:element ref="RestrictedPassword"/>
1369             </xs:sequence>
1370             <xs:attribute name="preauth" type="xs:integer" use="optional"/>
1371         </xs:restriction>
1372     </xs:complexContent>
1373 </xs:complexType>
1374
1375 <xs:complexType name="AuthenticatorBaseType">
1376     <xs:complexContent>
1377         <xs:restriction base="AuthenticatorBaseType">
1378             <xs:sequence>
1379                 <xs:element ref="SharedSecretChallengeResponse"/>
1380             </xs:sequence>
1381         </xs:restriction>
1382     </xs:complexContent>
1383 </xs:complexType>
1384
1385 <xs:complexType name="SharedSecretChallengeResponseType">
1386     <xs:complexContent>
1387         <xs:restriction base="SharedSecretChallengeResponseType">
1388             <xs:attribute name="method" type="xs:anyURI"
1389 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
1390         </xs:restriction>
1391     </xs:complexContent>
1392 </xs:complexType>
1393
1394 </xs:redefine>
1395
1396 </xs:schema>
1397

```

1398 An example of an XML instance conforming to this class schema is as follows:

```
1399 <AuthenticationContextDeclaration
1400   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos">
1401
1402   <AuthnMethod>
1403
1404     <PrincipalAuthenticationMechanism preauth="0">
1405       <RestrictedPassword>
1406         <Length min="4"/>
1407       </RestrictedPassword>
1408     </PrincipalAuthenticationMechanism>
1409
1410     <Authenticator>
1411       <AuthenticatorSequence>
1412         <SharedSecretChallengeResponse
1413   method="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
1414       </AuthenticatorSequence>
1415     </Authenticator>
1416
1417   </AuthnMethod>
1418
1419 </AuthenticationContextDeclaration>
```

1420 **3.4.4 MobileOneFactorUnregistered**

1421 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered

1422 Note that this URI is also used as the target namespace in the corresponding authentication context class
1423 schema document ([SAMLAC-MOFU]).

1424 Reflects no mobile customer registration procedures and an authentication of the mobile device without
1425 requiring explicit end-user interaction. This context class authenticates only the device and never the user;
1426 it is useful when services other than the mobile operator want to add a secure device authentication to
1427 their authentication process.

```
1428 <?xml version="1.0" encoding="UTF-8"?>
1429
1430 <xs:schema
1431   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregi
1432   stered"
1433   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1434   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered"
1435   finalDefault="extension"
1436   blockDefault="substitution"
1437   version="2.0">
1438
1439   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
1440
1441     <xs:annotation>
1442       <xs:documentation>
1443         Class identifier:
1444   urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
1445         Document identifier: sstc-saml-schema-authn-context-mobileonefactor-
1446   unreg-2.0
1447         Location: http://www.oasis-
1448   open.org/committees/documents.php?wg_abbrev=security
1449         Revision history:
1450           V2.0 CD-04 (January, 2005):
1451             New authentication context class schema for SAML V2.0.
1452       </xs:documentation>
1453     </xs:annotation>
1454
1455     <xs:complexType name="AuthnContextDeclarationBaseType">
1456       <xs:complexContent>
1457         <xs:restriction base="AuthnContextDeclarationBaseType">
```

```

1458     <xs:sequence>
1459         <xs:element ref="Identification" minOccurs="0"/>
1460         <xs:element ref="TechnicalProtection" minOccurs="0"/>
1461         <xs:element ref="OperationalProtection" minOccurs="0"/>
1462         <xs:element ref="AuthnMethod"/>
1463         <xs:element ref="GoverningAgreements" minOccurs="0"/>
1464         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1465     </xs:sequence>
1466     <xs:attribute name="ID" type="xs:ID" use="optional"/>
1467 </xs:restriction>
1468 </xs:complexContent>
1469 </xs:complexType>
1470
1471 <xs:complexType name="AuthnMethodBaseType">
1472     <xs:complexContent>
1473         <xs:restriction base="AuthnMethodBaseType">
1474             <xs:sequence>
1475                 <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1476                 <xs:element ref="Authenticator"/>
1477                 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1478                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1479             </xs:sequence>
1480         </xs:restriction>
1481     </xs:complexContent>
1482 </xs:complexType>
1483
1484 <xs:complexType name="AuthenticatorBaseType">
1485     <xs:complexContent>
1486         <xs:restriction base="AuthenticatorBaseType">
1487             <xs:sequence>
1488                 <xs:choice>
1489                     <xs:element ref="DigSig"/>
1490                     <xs:element ref="ZeroKnowledge"/>
1491                     <xs:element ref="SharedSecretChallengeResponse"/>
1492                     <xs:element ref="SharedSecretDynamicPlaintext"/>
1493                     <xs:element ref="AsymmetricDecryption"/>
1494                     <xs:element ref="AsymmetricKeyAgreement"/>
1495                 </xs:choice>
1496                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1497             </xs:sequence>
1498         </xs:restriction>
1499     </xs:complexContent>
1500 </xs:complexType>
1501
1502 <xs:complexType name="AuthenticatorTransportProtocolType">
1503     <xs:complexContent>
1504         <xs:restriction base="AuthenticatorTransportProtocolType">
1505             <xs:sequence>
1506                 <xs:choice>
1507                     <xs:element ref="SSL"/>
1508                     <xs:element ref="MobileNetworkNoEncryption"/>
1509                     <xs:element ref="MobileNetworkRadioEncryption"/>
1510                     <xs:element ref="MobileNetworkEndToEndEncryption"/>
1511                     <xs:element ref="WTLS"/>
1512                 </xs:choice>
1513                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1514             </xs:sequence>
1515         </xs:restriction>
1516     </xs:complexContent>
1517 </xs:complexType>
1518
1519 <xs:complexType name="OperationalProtectionType">
1520     <xs:complexContent>
1521         <xs:restriction base="OperationalProtectionType">
1522             <xs:sequence>
1523                 <xs:element ref="SecurityAudit"/>
1524                 <xs:element ref="DeactivationCallCenter"/>

```

```

1525         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1526     </xs:sequence>
1527 </xs:restriction>
1528 </xs:complexContent>
1529 </xs:complexType>
1530
1531 <xs:complexType name="TechnicalProtectionBaseType">
1532     <xs:complexContent>
1533         <xs:restriction base="TechnicalProtectionBaseType">
1534             <xs:sequence>
1535                 <xs:choice>
1536                     <xs:element ref="PrivateKeyProtection"/>
1537                     <xs:element ref="SecretKeyProtection"/>
1538                 </xs:choice>
1539                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1540             </xs:sequence>
1541         </xs:restriction>
1542     </xs:complexContent>
1543 </xs:complexType>
1544
1545 <xs:complexType name="PrivateKeyProtectionType">
1546     <xs:complexContent>
1547         <xs:restriction base="PrivateKeyProtectionType">
1548             <xs:sequence>
1549                 <xs:element ref="KeyStorage"/>
1550                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1551             </xs:sequence>
1552         </xs:restriction>
1553     </xs:complexContent>
1554 </xs:complexType>
1555
1556 <xs:complexType name="SecretKeyProtectionType">
1557     <xs:complexContent>
1558         <xs:restriction base="SecretKeyProtectionType">
1559             <xs:sequence>
1560                 <xs:element ref="KeyStorage"/>
1561                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1562             </xs:sequence>
1563         </xs:restriction>
1564     </xs:complexContent>
1565 </xs:complexType>
1566
1567 <xs:complexType name="KeyStorageType">
1568     <xs:complexContent>
1569         <xs:restriction base="KeyStorageType">
1570             <xs:attribute name="medium" use="required">
1571                 <xs:simpleType>
1572                     <xs:restriction base="mediumType">
1573                         <xs:enumeration value="MobileDevice"/>
1574                         <xs:enumeration value="MobileAuthCard"/>
1575                         <xs:enumeration value="smartcard"/>
1576                     </xs:restriction>
1577                 </xs:simpleType>
1578             </xs:attribute>
1579         </xs:restriction>
1580     </xs:complexContent>
1581 </xs:complexType>
1582
1583 <xs:complexType name="SecurityAuditType">
1584     <xs:complexContent>
1585         <xs:restriction base="SecurityAuditType">
1586             <xs:sequence>
1587                 <xs:element ref="SwitchAudit"/>
1588                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1589             </xs:sequence>
1590         </xs:restriction>
1591     </xs:complexContent>

```

```

1592     </xs:complexType>
1593
1594     <xs:complexType name="IdentificationType">
1595       <xs:complexContent>
1596         <xs:restriction base="IdentificationType">
1597           <xs:sequence>
1598             <xs:element ref="GoverningAgreements"/>
1599             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1600           </xs:sequence>
1601           <xs:attribute name="nym">
1602             <xs:simpleType>
1603               <xs:restriction base="nymType">
1604                 <xs:enumeration value="anonymity"/>
1605                 <xs:enumeration value="pseudonymity"/>
1606               </xs:restriction>
1607             </xs:simpleType>
1608           </xs:attribute>
1609         </xs:restriction>
1610       </xs:complexContent>
1611     </xs:complexType>
1612
1613   </xs:redefine>
1614
1615 </xs:schema>

```

1616 3.4.5 MobileTwoFactorUnregistered

1617 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered

1618 Note that this URI is also used as the target namespace in the corresponding authentication context class
 1619 schema document ([SAMLAC-MTFU]).

1620 Reflects no mobile customer registration procedures and a two-factor based authentication, such as
 1621 secure device and user PIN. This context class is useful when a service other than the mobile operator
 1622 wants to link their customer ID to a mobile supplied two-factor authentication service by capturing mobile
 1623 phone data at enrollment.

```

1624 <?xml version="1.0" encoding="UTF-8"?>
1625
1626 <xs:schema
1627   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregist
1628   ered"
1629   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1630   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered"
1631   finalDefault="extension"
1632   blockDefault="substitution"
1633   version="2.0">
1634
1635   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
1636
1637     <xs:annotation>
1638       <xs:documentation>
1639         Class identifier:
1640         urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
1641         Document identifier: sstc-saml-schema-authn-context-mobiletwofactor-
1642         unreg-2.0
1643         Location: http://www.oasis-
1644         open.org/committees/documents.php?wg_abbrev=security
1645         Revision history:
1646         V2.0 CD-04 (January, 2005):
1647         New authentication context class schema for SAML V2.0.
1648       </xs:documentation>
1649     </xs:annotation>
1650
1651     <xs:complexType name="AuthnContextDeclarationBaseType">
1652       <xs:complexContent>

```

```

1653     <xs:restriction base="AuthnContextDeclarationBaseType">
1654       <xs:sequence>
1655         <xs:element ref="Identification" minOccurs="0"/>
1656         <xs:element ref="TechnicalProtection" minOccurs="0"/>
1657         <xs:element ref="OperationalProtection" minOccurs="0"/>
1658         <xs:element ref="AuthnMethod"/>
1659         <xs:element ref="GoverningAgreements" minOccurs="0"/>
1660         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1661       </xs:sequence>
1662       <xs:attribute name="ID" type="xs:ID" use="optional"/>
1663     </xs:restriction>
1664   </xs:complexContent>
1665 </xs:complexType>
1666
1667 <xs:complexType name="AuthnMethodBaseType">
1668   <xs:complexContent>
1669     <xs:restriction base="AuthnMethodBaseType">
1670       <xs:sequence>
1671         <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1672         <xs:element ref="Authenticator"/>
1673         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1674         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1675       </xs:sequence>
1676     </xs:restriction>
1677   </xs:complexContent>
1678 </xs:complexType>
1679
1680 <xs:complexType name="AuthenticatorBaseType">
1681   <xs:complexContent>
1682     <xs:restriction base="AuthenticatorBaseType">
1683       <xs:sequence>
1684         <xs:choice>
1685           <xs:element ref="DigSig"/>
1686           <xs:element ref="ZeroKnowledge"/>
1687           <xs:element ref="SharedSecretChallengeResponse"/>
1688           <xs:element ref="SharedSecretDynamicPlaintext"/>
1689           <xs:element ref="AsymmetricDecryption"/>
1690           <xs:element ref="AsymmetricKeyAgreement"/>
1691           <xs:element ref="ComplexAuthenticator"/>
1692         </xs:choice>
1693         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1694       </xs:sequence>
1695     </xs:restriction>
1696   </xs:complexContent>
1697 </xs:complexType>
1698
1699 <xs:complexType name="ComplexAuthenticatorType">
1700   <xs:complexContent>
1701     <xs:restriction base="ComplexAuthenticatorType">
1702       <xs:sequence>
1703         <xs:choice>
1704           <xs:element ref="SharedSecretChallengeResponse"/>
1705           <xs:element ref="SharedSecretDynamicPlaintext"/>
1706         </xs:choice>
1707         <xs:element ref="Password"/>
1708       </xs:sequence>
1709     </xs:restriction>
1710   </xs:complexContent>
1711 </xs:complexType>
1712
1713 <xs:complexType name="AuthenticatorTransportProtocolType">
1714   <xs:complexContent>
1715     <xs:restriction base="AuthenticatorTransportProtocolType">
1716       <xs:sequence>
1717         <xs:choice>
1718           <xs:element ref="SSL"/>
1719           <xs:element ref="MobileNetworkNoEncryption"/>

```

```

1720         <xs:element ref="MobileNetworkRadioEncryption"/>
1721         <xs:element ref="MobileNetworkEndToEndEncryption"/>
1722         <xs:element ref="WTLS"/>
1723     </xs:choice>
1724     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1725 </xs:sequence>
1726 </xs:restriction>
1727 </xs:complexContent>
1728 </xs:complexType>
1729
1730 <xs:complexType name="OperationalProtectionType">
1731     <xs:complexContent>
1732     <xs:restriction base="OperationalProtectionType">
1733     <xs:sequence>
1734     <xs:element ref="SecurityAudit"/>
1735     <xs:element ref="DeactivationCallCenter"/>
1736     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1737     </xs:sequence>
1738     </xs:restriction>
1739     </xs:complexContent>
1740 </xs:complexType>
1741
1742 <xs:complexType name="TechnicalProtectionBaseType">
1743     <xs:complexContent>
1744     <xs:restriction base="TechnicalProtectionBaseType">
1745     <xs:sequence>
1746     <xs:choice>
1747     <xs:element ref="PrivateKeyProtection"/>
1748     <xs:element ref="SecretKeyProtection"/>
1749     </xs:choice>
1750     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1751     </xs:sequence>
1752     </xs:restriction>
1753     </xs:complexContent>
1754 </xs:complexType>
1755
1756 <xs:complexType name="PrivateKeyProtectionType">
1757     <xs:complexContent>
1758     <xs:restriction base="PrivateKeyProtectionType">
1759     <xs:sequence>
1760     <xs:element ref="KeyActivation"/>
1761     <xs:element ref="KeyStorage"/>
1762     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1763     </xs:sequence>
1764     </xs:restriction>
1765     </xs:complexContent>
1766 </xs:complexType>
1767
1768 <xs:complexType name="SecretKeyProtectionType">
1769     <xs:complexContent>
1770     <xs:restriction base="SecretKeyProtectionType">
1771     <xs:sequence>
1772     <xs:element ref="KeyActivation"/>
1773     <xs:element ref="KeyStorage"/>
1774     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1775     </xs:sequence>
1776     </xs:restriction>
1777     </xs:complexContent>
1778 </xs:complexType>
1779
1780 <xs:complexType name="KeyStorageType">
1781     <xs:complexContent>
1782     <xs:restriction base="KeyStorageType">
1783     <xs:attribute name="medium" use="required">
1784     <xs:simpleType>
1785     <xs:restriction base="mediumType">
1786     <xs:enumeration value="MobileDevice"/>

```



```

1787         <xs:enumeration value="MobileAuthCard"/>
1788         <xs:enumeration value="smartcard"/>
1789     </xs:restriction>
1790 </xs:simpleType>
1791 </xs:attribute>
1792 </xs:restriction>
1793 </xs:complexContent>
1794 </xs:complexType>
1795
1796 <xs:complexType name="SecurityAuditType">
1797     <xs:complexContent>
1798         <xs:restriction base="SecurityAuditType">
1799             <xs:sequence>
1800                 <xs:element ref="SwitchAudit"/>
1801                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1802             </xs:sequence>
1803         </xs:restriction>
1804     </xs:complexContent>
1805 </xs:complexType>
1806
1807 <xs:complexType name="IdentificationType">
1808     <xs:complexContent>
1809         <xs:restriction base="IdentificationType">
1810             <xs:sequence>
1811                 <xs:element ref="GoverningAgreements"/>
1812                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1813             </xs:sequence>
1814             <xs:attribute name="nym">
1815                 <xs:simpleType>
1816                     <xs:restriction base="nymType">
1817                         <xs:enumeration value="anonymity"/>
1818                         <xs:enumeration value="pseudonymity"/>
1819                     </xs:restriction>
1820                 </xs:simpleType>
1821             </xs:attribute>
1822         </xs:restriction>
1823     </xs:complexContent>
1824 </xs:complexType>
1825
1826 </xs:redefine>
1827
1828 </xs:schema>

```

1829 3.4.6 MobileOneFactorContract

1830 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract

1831 Note that this URI is also used as the target namespace in the corresponding authentication context class
1832 schema document ([SAMLAC-MOFC]).

1833 Reflects mobile contract customer registration procedures and a single factor authentication. For example,
1834 a digital signing device with tamper resistant memory for key storage, such as the mobile MSISDN, but no
1835 required PIN or biometric for real-time user authentication.

```

1836 <?xml version="1.0" encoding="UTF-8"?>
1837
1838 <xs:schema
1839     targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
1840 >
1841     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1842     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
1843     finalDefault="extension"
1844     blockDefault="substitution"
1845     version="2.0">
1846
1847     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">

```

```

1848
1849     <xs:annotation>
1850     <xs:documentation>
1851         Class identifier:
1852 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
1853         Document identifier: sstc-saml-schema-authn-context-mobileonefactor-
1854 reg-2.0
1855         Location: http://www.oasis-
1856 open.org/committees/documents.php?wg_abbrev=security
1857         Revision history:
1858             V2.0 CD-04 (January, 2005):
1859             New authentication context class schema for SAML V2.0.
1860     </xs:documentation>
1861 </xs:annotation>
1862
1863 <xs:complexType name="AuthnContextDeclarationBaseType">
1864     <xs:complexContent>
1865     <xs:restriction base="AuthnContextDeclarationBaseType">
1866     <xs:sequence>
1867     <xs:element ref="Identification" minOccurs="0"/>
1868     <xs:element ref="TechnicalProtection" minOccurs="0"/>
1869     <xs:element ref="OperationalProtection" minOccurs="0"/>
1870     <xs:element ref="AuthnMethod"/>
1871     <xs:element ref="GoverningAgreements" minOccurs="0"/>
1872     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1873     </xs:sequence>
1874     <xs:attribute name="ID" type="xs:ID" use="optional"/>
1875     </xs:restriction>
1876 </xs:complexContent>
1877 </xs:complexType>
1878
1879 <xs:complexType name="AuthnMethodBaseType">
1880     <xs:complexContent>
1881     <xs:restriction base="AuthnMethodBaseType">
1882     <xs:sequence>
1883     <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1884     <xs:element ref="Authenticator"/>
1885     <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1886     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1887     </xs:sequence>
1888     </xs:restriction>
1889 </xs:complexContent>
1890 </xs:complexType>
1891
1892 <xs:complexType name="AuthenticatorBaseType">
1893     <xs:complexContent>
1894     <xs:restriction base="AuthenticatorBaseType">
1895     <xs:sequence>
1896     <xs:choice>
1897     <xs:element ref="DigSig"/>
1898     <xs:element ref="ZeroKnowledge"/>
1899     <xs:element ref="SharedSecretChallengeResponse"/>
1900     <xs:element ref="SharedSecretDynamicPlaintext"/>
1901     <xs:element ref="AsymmetricDecryption"/>
1902     <xs:element ref="AsymmetricKeyAgreement"/>
1903     </xs:choice>
1904     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1905     </xs:sequence>
1906     </xs:restriction>
1907 </xs:complexContent>
1908 </xs:complexType>
1909
1910 <xs:complexType name="AuthenticatorTransportProtocolType">
1911     <xs:complexContent>
1912     <xs:restriction base="AuthenticatorTransportProtocolType">
1913     <xs:sequence>
1914     <xs:choice>

```

```

1915         <xs:element ref="SSL"/>
1916         <xs:element ref="MobileNetworkNoEncryption"/>
1917         <xs:element ref="MobileNetworkRadioEncryption"/>
1918         <xs:element ref="MobileNetworkEndToEndEncryption"/>
1919         <xs:element ref="WTLS"/>
1920     </xs:choice>
1921     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1922 </xs:sequence>
1923 </xs:restriction>
1924 </xs:complexContent>
1925 </xs:complexType>
1926
1927 <xs:complexType name="OperationalProtectionType">
1928     <xs:complexContent>
1929         <xs:restriction base="OperationalProtectionType">
1930             <xs:sequence>
1931                 <xs:element ref="SecurityAudit"/>
1932                 <xs:element ref="DeactivationCallCenter"/>
1933                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1934             </xs:sequence>
1935         </xs:restriction>
1936     </xs:complexContent>
1937 </xs:complexType>
1938
1939 <xs:complexType name="TechnicalProtectionBaseType">
1940     <xs:complexContent>
1941         <xs:restriction base="TechnicalProtectionBaseType">
1942             <xs:sequence>
1943                 <xs:choice>
1944                     <xs:element ref="PrivateKeyProtection"/>
1945                     <xs:element ref="SecretKeyProtection"/>
1946                 </xs:choice>
1947                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1948             </xs:sequence>
1949         </xs:restriction>
1950     </xs:complexContent>
1951 </xs:complexType>
1952
1953 <xs:complexType name="PrivateKeyProtectionType">
1954     <xs:complexContent>
1955         <xs:restriction base="PrivateKeyProtectionType">
1956             <xs:sequence>
1957                 <xs:element ref="KeyStorage"/>
1958                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1959             </xs:sequence>
1960         </xs:restriction>
1961     </xs:complexContent>
1962 </xs:complexType>
1963
1964 <xs:complexType name="SecretKeyProtectionType">
1965     <xs:complexContent>
1966         <xs:restriction base="SecretKeyProtectionType">
1967             <xs:sequence>
1968                 <xs:element ref="KeyStorage"/>
1969                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1970             </xs:sequence>
1971         </xs:restriction>
1972     </xs:complexContent>
1973 </xs:complexType>
1974
1975 <xs:complexType name="KeyStorageType">
1976     <xs:complexContent>
1977         <xs:restriction base="KeyStorageType">
1978             <xs:attribute name="medium" use="required">
1979                 <xs:simpleType>
1980                     <xs:restriction base="mediumType">
1981                         <xs:enumeration value="smartcard"/>

```

```

1982         <xs:enumeration value="MobileDevice"/>
1983         <xs:enumeration value="MobileAuthCard"/>
1984     </xs:restriction>
1985 </xs:simpleType>
1986 </xs:attribute>
1987 </xs:restriction>
1988 </xs:complexContent>
1989 </xs:complexType>
1990
1991 <xs:complexType name="SecurityAuditType">
1992     <xs:complexContent>
1993         <xs:restriction base="SecurityAuditType">
1994             <xs:sequence>
1995                 <xs:element ref="SwitchAudit"/>
1996                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1997             </xs:sequence>
1998         </xs:restriction>
1999     </xs:complexContent>
2000 </xs:complexType>
2001
2002 <xs:complexType name="IdentificationType">
2003     <xs:complexContent>
2004         <xs:restriction base="IdentificationType">
2005             <xs:sequence>
2006                 <xs:element ref="PhysicalVerification"/>
2007                 <xs:element ref="WrittenConsent"/>
2008                 <xs:element ref="GoverningAgreements"/>
2009                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2010             </xs:sequence>
2011             <xs:attribute name="nym">
2012                 <xs:simpleType>
2013                     <xs:restriction base="nymType">
2014                         <xs:enumeration value="anonymity"/>
2015                         <xs:enumeration value="verinymity"/>
2016                         <xs:enumeration value="pseudonymity"/>
2017                     </xs:restriction>
2018                 </xs:simpleType>
2019             </xs:attribute>
2020         </xs:restriction>
2021     </xs:complexContent>
2022 </xs:complexType>
2023
2024 </xs:redefine>
2025
2026 </xs:schema>

```

2027 3.4.7 MobileTwoFactorContract

2028 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract

2029 (Note that this URI is also used as the target namespace in the corresponding authentication context class
2030 schema document ([SAMLAC-MTFC]).

2031 Reflects mobile contract customer registration procedures and a two-factor based authentication. For
2032 example, a digital signing device with tamper resistant memory for key storage, such as a GSM SIM, that
2033 requires explicit proof of user identity and intent, such as a PIN or biometric.

```

2034 <?xml version="1.0" encoding="UTF-8"?>
2035
2036 <xs:schema
2037     targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
2038     xmlns:xs="http://www.w3.org/2001/XMLSchema"
2039     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
2040     finalDefault="extension"
2041     blockDefault="substitution"
2042     version="2.0">

```

```

2043
2044 <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2045
2046 <xs:annotation>
2047 <xs:documentation>
2048 Class identifier:
2049 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
2050 Document identifier: sstc-saml-schema-authn-context-mobiletwofactor-
2051 reg-2.0
2052 Location: http://www.oasis-
2053 open.org/committees/documents.php?wg_abbrev=security
2054 Revision history:
2055 V2.0 CD-04 (January, 2005):
2056 New authentication context class schema for SAML V2.0.
2057 </xs:documentation>
2058 </xs:annotation>
2059
2060 <xs:complexType name="AuthnContextDeclarationBaseType">
2061 <xs:complexContent>
2062 <xs:restriction base="AuthnContextDeclarationBaseType">
2063 <xs:sequence>
2064 <xs:element ref="Identification" minOccurs="0"/>
2065 <xs:element ref="TechnicalProtection" minOccurs="0"/>
2066 <xs:element ref="OperationalProtection" minOccurs="0"/>
2067 <xs:element ref="AuthnMethod"/>
2068 <xs:element ref="GoverningAgreements" minOccurs="0"/>
2069 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2070 </xs:sequence>
2071 <xs:attribute name="ID" type="xs:ID" use="optional"/>
2072 </xs:restriction>
2073 </xs:complexContent>
2074 </xs:complexType>
2075
2076 <xs:complexType name="AuthnMethodBaseType">
2077 <xs:complexContent>
2078 <xs:restriction base="AuthnMethodBaseType">
2079 <xs:sequence>
2080 <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
2081 <xs:element ref="Authenticator"/>
2082 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2083 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2084 </xs:sequence>
2085 </xs:restriction>
2086 </xs:complexContent>
2087 </xs:complexType>
2088
2089 <xs:complexType name="AuthenticatorBaseType">
2090 <xs:complexContent>
2091 <xs:restriction base="AuthenticatorBaseType">
2092 <xs:sequence>
2093 <xs:choice>
2094 <xs:element ref="DigSig"/>
2095 <xs:element ref="ZeroKnowledge"/>
2096 <xs:element ref="SharedSecretChallengeResponse"/>
2097 <xs:element ref="SharedSecretDynamicPlaintext"/>
2098 <xs:element ref="AsymmetricDecryption"/>
2099 <xs:element ref="AsymmetricKeyAgreement"/>
2100 <xs:element ref="ComplexAuthenticator"/>
2101 </xs:choice>
2102 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2103 </xs:sequence>
2104 </xs:restriction>
2105 </xs:complexContent>
2106 </xs:complexType>
2107
2108 <xs:complexType name="ComplexAuthenticatorType">
2109 <xs:complexContent>

```

```

2110     <xs:restriction base="ComplexAuthenticatorType">
2111         <xs:sequence>
2112             <xs:choice>
2113                 <xs:element ref="SharedSecretChallengeResponse"/>
2114                 <xs:element ref="SharedSecretDynamicPlaintext"/>
2115             </xs:choice>
2116             <xs:element ref="Password"/>
2117         </xs:sequence>
2118     </xs:restriction>
2119 </xs:complexContent>
2120 </xs:complexType>
2121
2122 <xs:complexType name="AuthenticatorTransportProtocolType">
2123     <xs:complexContent>
2124         <xs:restriction base="AuthenticatorTransportProtocolType">
2125             <xs:sequence>
2126                 <xs:choice>
2127                     <xs:element ref="SSL"/>
2128                     <xs:element ref="MobileNetworkNoEncryption"/>
2129                     <xs:element ref="MobileNetworkRadioEncryption"/>
2130                     <xs:element ref="MobileNetworkEndToEndEncryption"/>
2131                     <xs:element ref="WTLS"/>
2132                 </xs:choice>
2133                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2134             </xs:sequence>
2135         </xs:restriction>
2136     </xs:complexContent>
2137 </xs:complexType>
2138
2139 <xs:complexType name="OperationalProtectionType">
2140     <xs:complexContent>
2141         <xs:restriction base="OperationalProtectionType">
2142             <xs:sequence>
2143                 <xs:element ref="SecurityAudit"/>
2144                 <xs:element ref="DeactivationCallCenter"/>
2145                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2146             </xs:sequence>
2147         </xs:restriction>
2148     </xs:complexContent>
2149 </xs:complexType>
2150
2151 <xs:complexType name="TechnicalProtectionBaseType">
2152     <xs:complexContent>
2153         <xs:restriction base="TechnicalProtectionBaseType">
2154             <xs:sequence>
2155                 <xs:choice>
2156                     <xs:element ref="PrivateKeyProtection"/>
2157                     <xs:element ref="SecretKeyProtection"/>
2158                 </xs:choice>
2159                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2160             </xs:sequence>
2161         </xs:restriction>
2162     </xs:complexContent>
2163 </xs:complexType>
2164
2165 <xs:complexType name="PrivateKeyProtectionType">
2166     <xs:complexContent>
2167         <xs:restriction base="PrivateKeyProtectionType">
2168             <xs:sequence>
2169                 <xs:element ref="KeyActivation"/>
2170                 <xs:element ref="KeyStorage"/>
2171                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2172             </xs:sequence>
2173         </xs:restriction>
2174     </xs:complexContent>
2175 </xs:complexType>
2176

```

```

2177 <xs:complexType name="SecretKeyProtectionType">
2178 <xs:complexContent>
2179 <xs:restriction base="SecretKeyProtectionType">
2180 <xs:sequence>
2181 <xs:element ref="KeyActivation"/>
2182 <xs:element ref="KeyStorage"/>
2183 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2184 </xs:sequence>
2185 </xs:restriction>
2186 </xs:complexContent>
2187 </xs:complexType>
2188
2189 <xs:complexType name="KeyStorageType">
2190 <xs:complexContent>
2191 <xs:restriction base="KeyStorageType">
2192 <xs:attribute name="medium" use="required">
2193 <xs:simpleType>
2194 <xs:restriction base="mediumType">
2195 <xs:enumeration value="MobileDevice"/>
2196 <xs:enumeration value="MobileAuthCard"/>
2197 <xs:enumeration value="smartcard"/>
2198 </xs:restriction>
2199 </xs:simpleType>
2200 </xs:attribute>
2201 </xs:restriction>
2202 </xs:complexContent>
2203 </xs:complexType>
2204
2205 <xs:complexType name="SecurityAuditType">
2206 <xs:complexContent>
2207 <xs:restriction base="SecurityAuditType">
2208 <xs:sequence>
2209 <xs:element ref="SwitchAudit"/>
2210 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2211 </xs:sequence>
2212 </xs:restriction>
2213 </xs:complexContent>
2214 </xs:complexType>
2215
2216 <xs:complexType name="IdentificationType">
2217 <xs:complexContent>
2218 <xs:restriction base="IdentificationType">
2219 <xs:sequence>
2220 <xs:element ref="PhysicalVerification"/>
2221 <xs:element ref="WrittenConsent"/>
2222 <xs:element ref="GoverningAgreements"/>
2223 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2224 </xs:sequence>
2225 <xs:attribute name="nym">
2226 <xs:simpleType>
2227 <xs:restriction base="nymType">
2228 <xs:enumeration value="anonymity"/>
2229 <xs:enumeration value="verinymity"/>
2230 <xs:enumeration value="pseudonymity"/>
2231 </xs:restriction>
2232 </xs:simpleType>
2233 </xs:attribute>
2234 </xs:restriction>
2235 </xs:complexContent>
2236 </xs:complexType>
2237
2238 </xs:redefine>
2239
2240 </xs:schema>

```

2241 3.4.8 Password

2242 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes>Password

2243 Note that this URI is also used as the target namespace in the corresponding authentication context class
2244 schema document ([SAMLAC-Pass]).

2245 The Password class is applicable when a principal authenticates to an authentication authority through the
2246 presentation of a password over an unprotected HTTP session.

```
2247 <?xml version="1.0" encoding="UTF-8"?>
2248
2249 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes>Password"
2250   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2251   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes>Password"
2252   finalDefault="extension"
2253   blockDefault="substitution"
2254   version="2.0">
2255
2256   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2257
2258     <xs:annotation>
2259       <xs:documentation>
2260         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes>Password
2261         Document identifier: sstc-saml-schema-authn-context-pword-2.0
2262         Location: http://www.oasis-
2263 open.org/committees/documents.php?wg_abbrev=security
2264         Revision history:
2265           V2.0 CD-04 (January, 2005):
2266             New authentication context class schema for SAML V2.0.
2267       </xs:documentation>
2268     </xs:annotation>
2269
2270     <xs:complexType name="AuthnContextDeclarationBaseType">
2271       <xs:complexContent>
2272         <xs:restriction base="AuthnContextDeclarationBaseType">
2273           <xs:sequence>
2274             <xs:element ref="Identification" minOccurs="0"/>
2275             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2276             <xs:element ref="OperationalProtection" minOccurs="0"/>
2277             <xs:element ref="AuthnMethod"/>
2278             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2279             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2280           </xs:sequence>
2281           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2282         </xs:restriction>
2283       </xs:complexContent>
2284     </xs:complexType>
2285
2286     <xs:complexType name="AuthnMethodBaseType">
2287       <xs:complexContent>
2288         <xs:restriction base="AuthnMethodBaseType">
2289           <xs:sequence>
2290             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
2291             <xs:element ref="Authenticator"/>
2292             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2293             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2294           </xs:sequence>
2295         </xs:restriction>
2296       </xs:complexContent>
2297     </xs:complexType>
2298
2299     <xs:complexType name="AuthenticatorBaseType">
2300       <xs:complexContent>
2301         <xs:restriction base="AuthenticatorBaseType">
2302           <xs:sequence>
2303             <xs:element ref="RestrictedPassword"/>

```



```

2304         </xs:sequence>
2305     </xs:restriction>
2306 </xs:complexContent>
2307 </xs:complexType>
2308
2309 </xs:redefine>
2310
2311 </xs:schema>

```

2312 Following is an example of an XML instance that conforms to the context class schema:

```

2313 <AuthenticationContextDeclaration
2314   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password">
2315
2316   <AuthnMethod>
2317     <Authenticator>
2318       <AuthenticatorSequence>
2319         <RestrictedPassword>
2320           <Length min="4"/>
2321         </RestrictedPassword>
2322       </AuthenticatorSequence>
2323     </Authenticator>
2324   </AuthnMethod>
2325
2326 </AuthenticationContextDeclaration>

```

2327 3.4.9 PasswordProtectedTransport

2328 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

2329 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2330 schema document ([SAMLAC-PPT]).

2331 The PasswordProtectedTransport class is applicable when a principal authenticates to an authentication
 2332 authority through the presentation of a password over a protected session.

```

2333 <?xml version="1.0" encoding="UTF-8"?>
2334
2335 <xs:schema
2336   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp
2337   ort"
2338   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2339   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
2340   finalDefault="extension"
2341   blockDefault="substitution"
2342   version="2.0">
2343
2344   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2345
2346     <xs:annotation>
2347       <xs:documentation>
2348         Class identifier:
2349         urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
2350         Document identifier: sstc-saml-schema-authn-context-ppt-2.0
2351         Location: http://www.oasis-
2352         open.org/committees/documents.php?wg_abbrev=security
2353         Revision history:
2354         V2.0 CD-04 (January, 2005):
2355         New authentication context class schema for SAML V2.0.
2356       </xs:documentation>
2357     </xs:annotation>
2358
2359     <xs:complexType name="AuthnContextDeclarationBaseType">
2360       <xs:complexContent>
2361         <xs:restriction base="AuthnContextDeclarationBaseType">
2362           <xs:sequence>
2363             <xs:element ref="Identification" minOccurs="0"/>

```

```

2364     <xs:element ref="TechnicalProtection" minOccurs="0"/>
2365     <xs:element ref="OperationalProtection" minOccurs="0"/>
2366     <xs:element ref="AuthnMethod"/>
2367     <xs:element ref="GoverningAgreements" minOccurs="0"/>
2368     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2369   </xs:sequence>
2370   <xs:attribute name="ID" type="xs:ID" use="optional"/>
2371 </xs:restriction>
2372 </xs:complexContent>
2373 </xs:complexType>
2374
2375 <xs:complexType name="AuthnMethodBaseType">
2376   <xs:complexContent>
2377     <xs:restriction base="AuthnMethodBaseType">
2378       <xs:sequence>
2379         <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
2380         <xs:element ref="Authenticator"/>
2381         <xs:element ref="AuthenticatorTransportProtocol"/>
2382         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2383       </xs:sequence>
2384     </xs:restriction>
2385   </xs:complexContent>
2386 </xs:complexType>
2387
2388 <xs:complexType name="AuthenticatorBaseType">
2389   <xs:complexContent>
2390     <xs:restriction base="AuthenticatorBaseType">
2391       <xs:sequence>
2392         <xs:element ref="RestrictedPassword"/>
2393       </xs:sequence>
2394     </xs:restriction>
2395   </xs:complexContent>
2396 </xs:complexType>
2397
2398 <xs:complexType name="AuthenticatorTransportProtocolType">
2399   <xs:complexContent>
2400     <xs:restriction base="AuthenticatorTransportProtocolType">
2401       <xs:sequence>
2402         <xs:choice>
2403           <xs:element ref="SSL"/>
2404           <xs:element ref="MobileNetworkRadioEncryption"/>
2405           <xs:element ref="MobileNetworkEndToEndEncryption"/>
2406           <xs:element ref="WTLS"/>
2407           <xs:element ref="IPSec"/>
2408         </xs:choice>
2409         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2410       </xs:sequence>
2411     </xs:restriction>
2412   </xs:complexContent>
2413 </xs:complexType>
2414
2415 </xs:redefine>
2416
2417 </xs:schema>

```

2418 **3.4.10 PreviousSession**

2419 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession

2420 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2421 schema document ([SAMLAC-Prev]).

2422 The PreviousSession class is applicable when a principal had authenticated to an authentication authority
 2423 at some point in the past using any authentication context supported by that authentication authority.

2424 Consequently, a subsequent authentication event that the authentication authority will assert to the relying

2425 party may be significantly separated in time from the principal's current resource access request.

2426 The context for the previously authenticated session is explicitly not included in this context class because
2427 the user has not authenticated during this session, and so the mechanism that the user employed to
2428 authenticate in a previous session should not be used as part of a decision on whether to now allow
2429 access to a resource.

```
2430 <?xml version="1.0" encoding="UTF-8"?>
2431
2432 <xs:schema
2433 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2434 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2435 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2436 finalDefault="extension"
2437 blockDefault="substitution"
2438 version="2.0">
2439
2440 <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2441
2442 <xs:annotation>
2443 <xs:documentation>
2444 Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
2445 Document identifier: sstc-saml-schema-authn-context-session-2.0
2446 Location: http://www.oasis-
2447 open.org/committees/documents.php?wg_abbrev=security
2448 Revision history:
2449 V2.0 CD-04 (January, 2005):
2450 New authentication context class schema for SAML V2.0.
2451 </xs:documentation>
2452 </xs:annotation>
2453
2454 <xs:complexType name="AuthnContextDeclarationBaseType">
2455 <xs:complexContent>
2456 <xs:restriction base="AuthnContextDeclarationBaseType">
2457 <xs:sequence>
2458 <xs:element ref="Identification" minOccurs="0"/>
2459 <xs:element ref="TechnicalProtection" minOccurs="0"/>
2460 <xs:element ref="OperationalProtection" minOccurs="0"/>
2461 <xs:element ref="AuthnMethod"/>
2462 <xs:element ref="GoverningAgreements" minOccurs="0"/>
2463 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2464 </xs:sequence>
2465 <xs:attribute name="ID" type="xs:ID" use="optional"/>
2466 </xs:restriction>
2467 </xs:complexContent>
2468 </xs:complexType>
2469
2470 <xs:complexType name="AuthnMethodBaseType">
2471 <xs:complexContent>
2472 <xs:restriction base="AuthnMethodBaseType">
2473 <xs:sequence>
2474 <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
2475 <xs:element ref="Authenticator"/>
2476 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2477 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2478 </xs:sequence>
2479 </xs:restriction>
2480 </xs:complexContent>
2481 </xs:complexType>
2482
2483 <xs:complexType name="AuthenticatorBaseType">
2484 <xs:complexContent>
2485 <xs:restriction base="AuthenticatorBaseType">
2486 <xs:sequence>
2487 <xs:element ref="PreviousSession"/>
2488 </xs:sequence>
2489 </xs:restriction>
```

```
2490     </xs:complexContent>
2491     </xs:complexType>
2492
2493     </xs:redefine>
2494
2495 </xs:schema>
```

2496 3.4.11 Public Key – X.509

2497 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:X509

2498 Note that this URI is also used as the target namespace in the corresponding authentication context class
2499 schema document ([SAMLAC-X509]).

2500 The X509 context class indicates that the principal authenticated by means of a digital signature where the
2501 key was validated as part of an X.509 Public Key Infrastructure.

```
2502 <?xml version="1.0" encoding="UTF-8"?>
2503
2504 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2505     xmlns:xs="http://www.w3.org/2001/XMLSchema"
2506     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2507     finalDefault="extension"
2508     blockDefault="substitution"
2509     version="2.0">
2510
2511     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2512
2513         <xs:annotation>
2514             <xs:documentation>
2515                 Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:X509
2516                 Document identifier: sstc-saml-schema-authn-context-x509-2.0
2517                 Location: http://www.oasis-
2518 open.org/committees/documents.php?wg_abbrev=security
2519                 Revision history:
2520                 V2.0 CD-04 (January, 2005):
2521                 New authentication context class schema for SAML V2.0.
2522             </xs:documentation>
2523         </xs:annotation>
2524
2525         <xs:complexType name="AuthnContextDeclarationBaseType">
2526             <xs:complexContent>
2527                 <xs:restriction base="AuthnContextDeclarationBaseType">
2528                     <xs:sequence>
2529                         <xs:element ref="Identification" minOccurs="0"/>
2530                         <xs:element ref="TechnicalProtection" minOccurs="0"/>
2531                         <xs:element ref="OperationalProtection" minOccurs="0"/>
2532                         <xs:element ref="AuthnMethod"/>
2533                         <xs:element ref="GoverningAgreements" minOccurs="0"/>
2534                         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2535                     </xs:sequence>
2536                     <xs:attribute name="ID" type="xs:ID" use="optional"/>
2537                 </xs:restriction>
2538             </xs:complexContent>
2539         </xs:complexType>
2540
2541         <xs:complexType name="AuthnMethodBaseType">
2542             <xs:complexContent>
2543                 <xs:restriction base="AuthnMethodBaseType">
2544                     <xs:sequence>
2545                         <xs:element ref="PrincipalAuthenticationMechanism"/>
2546                         <xs:element ref="Authenticator"/>
2547                         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2548                         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2549                     </xs:sequence>
2550                 </xs:restriction>
```

```

2551     </xs:complexContent>
2552 </xs:complexType>
2553
2554 <xs:complexType name="PrincipalAuthenticationMechanismType">
2555   <xs:complexContent>
2556     <xs:restriction base="PrincipalAuthenticationMechanismType">
2557       <xs:sequence>
2558         <xs:element ref="RestrictedPassword"/>
2559       </xs:sequence>
2560       <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2561     </xs:restriction>
2562   </xs:complexContent>
2563 </xs:complexType>
2564
2565 <xs:complexType name="AuthenticatorBaseType">
2566   <xs:complexContent>
2567     <xs:restriction base="AuthenticatorBaseType">
2568       <xs:sequence>
2569         <xs:element ref="DigSig"/>
2570       </xs:sequence>
2571     </xs:restriction>
2572   </xs:complexContent>
2573 </xs:complexType>
2574
2575 <xs:complexType name="PublicKeyType">
2576   <xs:complexContent>
2577     <xs:restriction base="PublicKeyType">
2578       <xs:attribute name="keyValidation" type="xs:anyURI"
2579 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
2580     </xs:restriction>
2581   </xs:complexContent>
2582 </xs:complexType>
2583
2584 </xs:redefine>
2585
2586 </xs:schema>

```

2587 3.4.12 Public Key – PGP

2588 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PGP

2589 Note that this URI is also used as the target namespace in the corresponding authentication context class
2590 schema document ([SAMLAC-PGP]).

2591 The PGP context class indicates that the principal authenticated by means of a digital signature where the
2592 key was validated as part of a PGP Public Key Infrastructure.

```

2593 <?xml version="1.0" encoding="UTF-8"?>
2594
2595 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
2596   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2597   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
2598   finalDefault="extension"
2599   blockDefault="substitution"
2600   version="2.0">
2601
2602   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2603
2604     <xs:annotation>
2605       <xs:documentation>
2606         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
2607         Document identifier: sstc-saml-schema-authn-context-pgp-2.0
2608         Location: http://www.oasis-
2609 open.org/committees/documents.php?wg_abbrev=security
2610         Revision history:
2611         V2.0 CD-04 (January, 2005):

```

```

2612         New authentication context class schema for SAML V2.0.
2613     </xs:documentation>
2614 </xs:annotation>
2615
2616     <xs:complexType name="AuthnContextDeclarationBaseType">
2617         <xs:complexContent>
2618             <xs:restriction base="AuthnContextDeclarationBaseType">
2619                 <xs:sequence>
2620                     <xs:element ref="Identification" minOccurs="0"/>
2621                     <xs:element ref="TechnicalProtection" minOccurs="0"/>
2622                     <xs:element ref="OperationalProtection" minOccurs="0"/>
2623                     <xs:element ref="AuthnMethod"/>
2624                     <xs:element ref="GoverningAgreements" minOccurs="0"/>
2625                     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2626                 </xs:sequence>
2627                 <xs:attribute name="ID" type="xs:ID" use="optional"/>
2628             </xs:restriction>
2629         </xs:complexContent>
2630     </xs:complexType>
2631
2632     <xs:complexType name="AuthnMethodBaseType">
2633         <xs:complexContent>
2634             <xs:restriction base="AuthnMethodBaseType">
2635                 <xs:sequence>
2636                     <xs:element ref="PrincipalAuthenticationMechanism"/>
2637                     <xs:element ref="Authenticator"/>
2638                     <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2639                     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2640                 </xs:sequence>
2641             </xs:restriction>
2642         </xs:complexContent>
2643     </xs:complexType>
2644
2645     <xs:complexType name="PrincipalAuthenticationMechanismType">
2646         <xs:complexContent>
2647             <xs:restriction base="PrincipalAuthenticationMechanismType">
2648                 <xs:sequence>
2649                     <xs:element ref="RestrictedPassword"/>
2650                 </xs:sequence>
2651                 <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2652             </xs:restriction>
2653         </xs:complexContent>
2654     </xs:complexType>
2655
2656     <xs:complexType name="AuthenticatorBaseType">
2657         <xs:complexContent>
2658             <xs:restriction base="AuthenticatorBaseType">
2659                 <xs:sequence>
2660                     <xs:element ref="DigSig"/>
2661                 </xs:sequence>
2662             </xs:restriction>
2663         </xs:complexContent>
2664     </xs:complexType>
2665
2666     <xs:complexType name="PublicKeyType">
2667         <xs:complexContent>
2668             <xs:restriction base="PublicKeyType">
2669                 <xs:attribute name="keyValidation"
2670 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
2671             </xs:restriction>
2672         </xs:complexContent>
2673     </xs:complexType>
2674
2675 </xs:redefine>
2676
2677 </xs:schema>

```

2678 3.4.13 Public Key – SPKI

2679 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI

2680 Note that this URI is also used as the target namespace in the corresponding authentication context class
2681 schema document ([SAMLAC-SPKI]).

2682 The SPKI context class indicates that the principal authenticated by means of a digital signature where the
2683 key was validated via an SPKI Infrastructure.

```
2684 <?xml version="1.0" encoding="UTF-8"?>
2685
2686 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2687   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2688   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2689   finalDefault="extension"
2690   blockDefault="substitution"
2691   version="2.0">
2692
2693   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2694
2695     <xs:annotation>
2696       <xs:documentation>
2697         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
2698         Document identifier: sstc-saml-schema-authn-context-spki-2.0
2699         Location: http://www.oasis-
2700 open.org/committees/documents.php?wg_abbrev=security
2701         Revision history:
2702           V2.0 CD-04 (January, 2005):
2703             New authentication context class schema for SAML V2.0.
2704       </xs:documentation>
2705     </xs:annotation>
2706
2707     <xs:complexType name="AuthnContextDeclarationBaseType">
2708       <xs:complexContent>
2709         <xs:restriction base="AuthnContextDeclarationBaseType">
2710           <xs:sequence>
2711             <xs:element ref="Identification" minOccurs="0"/>
2712             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2713             <xs:element ref="OperationalProtection" minOccurs="0"/>
2714             <xs:element ref="AuthnMethod"/>
2715             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2716             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2717           </xs:sequence>
2718           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2719         </xs:restriction>
2720       </xs:complexContent>
2721     </xs:complexType>
2722
2723     <xs:complexType name="AuthnMethodBaseType">
2724       <xs:complexContent>
2725         <xs:restriction base="AuthnMethodBaseType">
2726           <xs:sequence>
2727             <xs:element ref="PrincipalAuthenticationMechanism"/>
2728             <xs:element ref="Authenticator"/>
2729             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2730             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2731           </xs:sequence>
2732         </xs:restriction>
2733       </xs:complexContent>
2734     </xs:complexType>
2735
2736     <xs:complexType name="PrincipalAuthenticationMechanismType">
2737       <xs:complexContent>
2738         <xs:restriction base="PrincipalAuthenticationMechanismType">
2739           <xs:sequence>
2740             <xs:element ref="RestrictedPassword"/>

```

```

2741     </xs:sequence>
2742     <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2743     </xs:restriction>
2744   </xs:complexContent>
2745 </xs:complexType>
2746
2747   <xs:complexType name="AuthenticatorBaseType">
2748     <xs:complexContent>
2749       <xs:restriction base="AuthenticatorBaseType">
2750         <xs:sequence>
2751           <xs:element ref="DigSig"/>
2752         </xs:sequence>
2753       </xs:restriction>
2754     </xs:complexContent>
2755   </xs:complexType>
2756
2757   <xs:complexType name="PublicKeyType">
2758     <xs:complexContent>
2759       <xs:restriction base="PublicKeyType">
2760         <xs:attribute name="keyValidation"
2761 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
2762       </xs:restriction>
2763     </xs:complexContent>
2764   </xs:complexType>
2765
2766 </xs:redefine>
2767
2768 </xs:schema>

```

2769 3.4.14 Public Key - XML Digital Signature

2770 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig

2771 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2772 schema document ([SAMLAC-XSig].

2773 This context class indicates that the principal authenticated by means of a digital signature according to
 2774 the processing rules specified in the XML Digital Signature specification [XMLSig].

```

2775 <?xml version="1.0" encoding="UTF-8"?>
2776
2777 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
2778   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2779   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
2780   finalDefault="extension"
2781   blockDefault="substitution"
2782   version="2.0">
2783
2784   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2785
2786     <xs:annotation>
2787       <xs:documentation>
2788         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
2789         Document identifier: sstc-saml-schema-authn-context-xmldsig-2.0
2790         Location: http://www.oasis-
2791 open.org/committees/documents.php?wg_abbrev=security
2792         Revision history:
2793           V2.0 CD-04 (January, 2005):
2794             New authentication context class schema for SAML V2.0.
2795       </xs:documentation>
2796     </xs:annotation>
2797
2798     <xs:complexType name="AuthnContextDeclarationBaseType">
2799       <xs:complexContent>
2800         <xs:restriction base="AuthnContextDeclarationBaseType">
2801           <xs:sequence>

```



```

2802     <xs:element ref="Identification" minOccurs="0"/>
2803     <xs:element ref="TechnicalProtection" minOccurs="0"/>
2804     <xs:element ref="OperationalProtection" minOccurs="0"/>
2805     <xs:element ref="AuthnMethod"/>
2806     <xs:element ref="GoverningAgreements" minOccurs="0"/>
2807     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2808   </xs:sequence>
2809   <xs:attribute name="ID" type="xs:ID" use="optional"/>
2810 </xs:restriction>
2811 </xs:complexContent>
2812 </xs:complexType>
2813
2814 <xs:complexType name="AuthnMethodBaseType">
2815   <xs:complexContent>
2816     <xs:restriction base="AuthnMethodBaseType">
2817       <xs:sequence>
2818         <xs:element ref="PrincipalAuthenticationMechanism"/>
2819         <xs:element ref="Authenticator"/>
2820         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2821         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2822       </xs:sequence>
2823     </xs:restriction>
2824   </xs:complexContent>
2825 </xs:complexType>
2826
2827 <xs:complexType name="PrincipalAuthenticationMechanismType">
2828   <xs:complexContent>
2829     <xs:restriction base="PrincipalAuthenticationMechanismType">
2830       <xs:sequence>
2831         <xs:element ref="RestrictedPassword"/>
2832       </xs:sequence>
2833       <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2834     </xs:restriction>
2835   </xs:complexContent>
2836 </xs:complexType>
2837
2838 <xs:complexType name="AuthenticatorBaseType">
2839   <xs:complexContent>
2840     <xs:restriction base="AuthenticatorBaseType">
2841       <xs:sequence>
2842         <xs:element ref="DigSig"/>
2843       </xs:sequence>
2844     </xs:restriction>
2845   </xs:complexContent>
2846 </xs:complexType>
2847
2848 <xs:complexType name="PublicKeyType">
2849   <xs:complexContent>
2850     <xs:restriction base="PublicKeyType">
2851       <xs:attribute name="keyValidation" type="xs:anyURI"
2852 fixed="urn:ietf:rfc:3075"/>
2853     </xs:restriction>
2854   </xs:complexContent>
2855 </xs:complexType>
2856
2857 </xs:redefine>
2858
2859 </xs:schema>

```

2860 3.4.15 Smartcard

2861 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard

2862 Note that this URI is also used as the target namespace in the corresponding authentication context class
2863 schema document ([SAMLAC-Smart]).

2864 The Smartcard class is identified when a principal authenticates to an authentication authority using a
2865 smartcard.

```
2866 <?xml version="1.0" encoding="UTF-8"?>
2867
2868 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
2869   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2870   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
2871   finalDefault="extension"
2872   blockDefault="substitution"
2873   version="2.0">
2874
2875   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2876
2877     <xs:annotation>
2878       <xs:documentation>
2879         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
2880         Document identifier: sstc-saml-schema-authn-context-smartcard-2.0
2881         Location: http://www.oasis-
2882 open.org/committees/documents.php?wg_abbrev=security
2883         Revision history:
2884           V2.0 CD-04 (January, 2005):
2885             New authentication context class schema for SAML V2.0.
2886       </xs:documentation>
2887     </xs:annotation>
2888
2889     <xs:complexType name="AuthnContextDeclarationBaseType">
2890       <xs:complexContent>
2891         <xs:restriction base="AuthnContextDeclarationBaseType">
2892           <xs:sequence>
2893             <xs:element ref="Identification" minOccurs="0"/>
2894             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2895             <xs:element ref="OperationalProtection" minOccurs="0"/>
2896             <xs:element ref="AuthnMethod"/>
2897             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2898             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2899           </xs:sequence>
2900           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2901         </xs:restriction>
2902       </xs:complexContent>
2903     </xs:complexType>
2904
2905     <xs:complexType name="AuthnMethodBaseType">
2906       <xs:complexContent>
2907         <xs:restriction base="AuthnMethodBaseType">
2908           <xs:sequence>
2909             <xs:element ref="PrincipalAuthenticationMechanism"/>
2910             <xs:element ref="Authenticator"/>
2911             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2912             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2913           </xs:sequence>
2914         </xs:restriction>
2915       </xs:complexContent>
2916     </xs:complexType>
2917
2918     <xs:complexType name="PrincipalAuthenticationMechanismType">
2919       <xs:complexContent>
2920         <xs:restriction base="PrincipalAuthenticationMechanismType">
2921           <xs:sequence>
2922             <xs:element ref="Smartcard"/>
2923           </xs:sequence>
2924         </xs:restriction>
2925       </xs:complexContent>
2926     </xs:complexType>
2927
2928   </xs:redefine>
2929
```

2930 </xs:schema>

2931 3.4.16 SmartcardPKI

2932 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

2933 Note that this URI is also used as the target namespace in the corresponding authentication context class
2934 schema document ([SAMLAC-SmPKI]).

2935 The SmartcardPKI class is applicable when a principal authenticates to an authentication authority through
2936 a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN.

```
2937 <?xml version="1.0" encoding="UTF-8"?>
2938
2939 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
2940   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2941   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
2942   finalDefault="extension"
2943   blockDefault="substitution"
2944   version="2.0">
2945
2946   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
2947
2948     <xs:annotation>
2949       <xs:documentation>
2950         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
2951         Document identifier: sstc-saml-schema-authn-context-smartcardpki-2.0
2952         Location: http://www.oasis-
2953 open.org/committees/documents.php?wg_abbrev=security
2954         Revision history:
2955           V2.0 CD-04 (January, 2005):
2956             New authentication context class schema for SAML V2.0.
2957       </xs:documentation>
2958     </xs:annotation>
2959
2960     <xs:complexType name="AuthnContextDeclarationBaseType">
2961       <xs:complexContent>
2962         <xs:restriction base="AuthnContextDeclarationBaseType">
2963           <xs:sequence>
2964             <xs:element ref="Identification" minOccurs="0"/>
2965             <xs:element ref="TechnicalProtection"/>
2966             <xs:element ref="OperationalProtection" minOccurs="0"/>
2967             <xs:element ref="AuthnMethod"/>
2968             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2969             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2970           </xs:sequence>
2971           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2972         </xs:restriction>
2973       </xs:complexContent>
2974     </xs:complexType>
2975
2976     <xs:complexType name="AuthnMethodBaseType">
2977       <xs:complexContent>
2978         <xs:restriction base="AuthnMethodBaseType">
2979           <xs:sequence>
2980             <xs:element ref="PrincipalAuthenticationMechanism"/>
2981             <xs:element ref="Authenticator"/>
2982             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2983             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2984           </xs:sequence>
2985         </xs:restriction>
2986       </xs:complexContent>
2987     </xs:complexType>
2988
2989     <xs:complexType name="TechnicalProtectionBaseType">
2990       <xs:complexContent>
```

```

2991     <xs:restriction base="TechnicalProtectionBaseType">
2992       <xs:sequence>
2993         <xs:choice>
2994           <xs:element ref="PrivateKeyProtection"/>
2995         </xs:choice>
2996       </xs:sequence>
2997     </xs:restriction>
2998   </xs:complexContent>
2999 </xs:complexType>
3000
3001 <xs:complexType name="PrincipalAuthenticationMechanismType">
3002   <xs:complexContent>
3003     <xs:restriction base="PrincipalAuthenticationMechanismType">
3004       <xs:sequence>
3005         <xs:element ref="Smartcard"/>
3006         <xs:element ref="ActivationPin"/>
3007         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3008       </xs:sequence>
3009     </xs:restriction>
3010   </xs:complexContent>
3011 </xs:complexType>
3012
3013 <xs:complexType name="AuthenticatorBaseType">
3014   <xs:complexContent>
3015     <xs:restriction base="AuthenticatorBaseType">
3016       <xs:sequence>
3017         <xs:choice>
3018           <xs:element ref="DigSig"/>
3019           <xs:element ref="AsymmetricDecryption"/>
3020           <xs:element ref="AsymmetricKeyAgreement"/>
3021         </xs:choice>
3022         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3023       </xs:sequence>
3024     </xs:restriction>
3025   </xs:complexContent>
3026 </xs:complexType>
3027
3028 <xs:complexType name="PrivateKeyProtectionType">
3029   <xs:complexContent>
3030     <xs:restriction base="PrivateKeyProtectionType">
3031       <xs:sequence>
3032         <xs:element ref="KeyActivation"/>
3033         <xs:element ref="KeyStorage"/>
3034         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3035       </xs:sequence>
3036     </xs:restriction>
3037   </xs:complexContent>
3038 </xs:complexType>
3039
3040 <xs:complexType name="KeyActivationType">
3041   <xs:complexContent>
3042     <xs:restriction base="KeyActivationType">
3043       <xs:sequence>
3044         <xs:element ref="ActivationPin"/>
3045       </xs:sequence>
3046     </xs:restriction>
3047   </xs:complexContent>
3048 </xs:complexType>
3049
3050 <xs:complexType name="KeyStorageType">
3051   <xs:complexContent>
3052     <xs:restriction base="KeyStorageType">
3053       <xs:attribute name="medium" use="required">
3054         <xs:simpleType>
3055           <xs:restriction base="mediumType">
3056             <xs:enumeration value="smartcard"/>
3057           </xs:restriction>

```

```
3058         </xs:simpleType>
3059     </xs:attribute>
3060 </xs:restriction>
3061 </xs:complexContent>
3062 </xs:complexType>
3063
3064 </xs:redefine>
3065
3066 </xs:schema>
```

3067 **3.4.17 SoftwarePKI**

3068 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI

3069 Note that this URI is also used as the target namespace in the corresponding authentication context class
3070 schema document ([SAMLAC-SwPKI]).

3071 The Software-PKI class is applicable when a principal uses an X.509 certificate stored in software to
3072 authenticate to the authentication authority.

```
3073 <?xml version="1.0" encoding="UTF-8"?>
3074
3075 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3076     xmlns:xs="http://www.w3.org/2001/XMLSchema"
3077     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3078     finalDefault="extension"
3079     blockDefault="substitution"
3080     version="2.0">
3081
3082     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3083
3084         <xs:annotation>
3085             <xs:documentation>
3086                 Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
3087                 Document identifier: sstc-saml-schema-authn-context-softwarepki-2.0
3088                 Location: http://www.oasis-
3089 open.org/committees/documents.php?wg_abbrev=security
3090                 Revision history:
3091                     V2.0 CD-04 (January, 2005):
3092                     New authentication context class schema for SAML V2.0.
3093             </xs:documentation>
3094         </xs:annotation>
3095
3096         <xs:complexType name="AuthnContextDeclarationBaseType">
3097             <xs:complexContent>
3098                 <xs:restriction base="AuthnContextDeclarationBaseType">
3099                     <xs:sequence>
3100                         <xs:element ref="Identification" minOccurs="0"/>
3101                         <xs:element ref="TechnicalProtection"/>
3102                         <xs:element ref="OperationalProtection" minOccurs="0"/>
3103                         <xs:element ref="AuthnMethod"/>
3104                         <xs:element ref="GoverningAgreements" minOccurs="0"/>
3105                         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3106                     </xs:sequence>
3107                     <xs:attribute name="ID" type="xs:ID" use="optional"/>
3108                 </xs:restriction>
3109             </xs:complexContent>
3110         </xs:complexType>
3111
3112         <xs:complexType name="AuthnMethodBaseType">
3113             <xs:complexContent>
3114                 <xs:restriction base="AuthnMethodBaseType">
3115                     <xs:sequence>
3116                         <xs:element ref="PrincipalAuthenticationMechanism"/>
3117                         <xs:element ref="Authenticator"/>
3118                         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
```

```

3119         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3120     </xs:sequence>
3121 </xs:restriction>
3122 </xs:complexContent>
3123 </xs:complexType>
3124
3125 <xs:complexType name="TechnicalProtectionBaseType">
3126     <xs:complexContent>
3127         <xs:restriction base="TechnicalProtectionBaseType">
3128             <xs:sequence>
3129                 <xs:choice>
3130                     <xs:element ref="PrivateKeyProtection"/>
3131                 </xs:choice>
3132             </xs:sequence>
3133         </xs:restriction>
3134     </xs:complexContent>
3135 </xs:complexType>
3136
3137 <xs:complexType name="PrincipalAuthenticationMechanismType">
3138     <xs:complexContent>
3139         <xs:restriction base="PrincipalAuthenticationMechanismType">
3140             <xs:sequence>
3141                 <xs:element ref="ActivationPin"/>
3142                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3143             </xs:sequence>
3144         </xs:restriction>
3145     </xs:complexContent>
3146 </xs:complexType>
3147
3148 <xs:complexType name="AuthenticatorBaseType">
3149     <xs:complexContent>
3150         <xs:restriction base="AuthenticatorBaseType">
3151             <xs:sequence>
3152                 <xs:choice>
3153                     <xs:element ref="DigSig"/>
3154                     <xs:element ref="AsymmetricDecryption"/>
3155                     <xs:element ref="AsymmetricKeyAgreement"/>
3156                 </xs:choice>
3157                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3158             </xs:sequence>
3159         </xs:restriction>
3160     </xs:complexContent>
3161 </xs:complexType>
3162
3163 <xs:complexType name="PrivateKeyProtectionType">
3164     <xs:complexContent>
3165         <xs:restriction base="PrivateKeyProtectionType">
3166             <xs:sequence>
3167                 <xs:element ref="KeyActivation"/>
3168                 <xs:element ref="KeyStorage"/>
3169                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3170             </xs:sequence>
3171         </xs:restriction>
3172     </xs:complexContent>
3173 </xs:complexType>
3174
3175 <xs:complexType name="KeyActivationType">
3176     <xs:complexContent>
3177         <xs:restriction base="KeyActivationType">
3178             <xs:sequence>
3179                 <xs:element ref="ActivationPin"/>
3180                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3181             </xs:sequence>
3182         </xs:restriction>
3183     </xs:complexContent>
3184 </xs:complexType>
3185

```

```

3186     <xs:complexType name="KeyStorageType">
3187       <xs:complexContent>
3188         <xs:restriction base="KeyStorageType">
3189           <xs:attribute name="medium" use="required">
3190             <xs:simpleType>
3191               <xs:restriction base="mediumType">
3192                 <xs:enumeration value="memory"/>
3193               </xs:restriction>
3194             </xs:simpleType>
3195           </xs:attribute>
3196         </xs:restriction>
3197       </xs:complexContent>
3198     </xs:complexType>
3199
3200 </xs:redefine>
3201
3202 </xs:schema>

```

3203 3.4.18 Telephony

3204 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony

3205 Note that this URI is also used as the target namespace in the corresponding authentication context class
3206 schema document ([SAMLAC-Tele]).

3207 This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone
3208 number, transported via a telephony protocol such as ADSL.

```

3209 <?xml version="1.0" encoding="UTF-8"?>
3210
3211 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3212   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3213   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3214   finalDefault="extension"
3215   blockDefault="substitution"
3216   version="2.0">
3217
3218   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3219
3220     <xs:annotation>
3221       <xs:documentation>
3222         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
3223         Document identifier: sstc-saml-schema-authn-context-telephony-2.0
3224         Location: http://www.oasis-
3225 open.org/committees/documents.php?wg_abbrev=security
3226         Revision history:
3227           V2.0 CD-04 (January, 2005):
3228             New authentication context class schema for SAML V2.0.
3229       </xs:documentation>
3230     </xs:annotation>
3231
3232     <xs:complexType name="AuthnContextDeclarationBaseType">
3233       <xs:complexContent>
3234         <xs:restriction base="AuthnContextDeclarationBaseType">
3235           <xs:sequence>
3236             <xs:element ref="Identification" minOccurs="0"/>
3237             <xs:element ref="TechnicalProtection" minOccurs="0"/>
3238             <xs:element ref="OperationalProtection" minOccurs="0"/>
3239             <xs:element ref="AuthnMethod"/>
3240             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3241             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3242           </xs:sequence>
3243           <xs:attribute name="ID" type="xs:ID" use="optional"/>
3244         </xs:restriction>
3245       </xs:complexContent>
3246     </xs:complexType>

```

```

3247
3248     <xs:complexType name="AuthnMethodBaseType">
3249       <xs:complexContent>
3250         <xs:restriction base="AuthnMethodBaseType">
3251           <xs:sequence>
3252             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3253             <xs:element ref="Authenticator"/>
3254             <xs:element ref="AuthenticatorTransportProtocol"/>
3255             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3256           </xs:sequence>
3257         </xs:restriction>
3258       </xs:complexContent>
3259     </xs:complexType>
3260
3261     <xs:complexType name="AuthenticatorBaseType">
3262       <xs:complexContent>
3263         <xs:restriction base="AuthenticatorBaseType">
3264           <xs:sequence>
3265             <xs:element ref="SubscriberLineNumber"/>
3266           </xs:sequence>
3267         </xs:restriction>
3268       </xs:complexContent>
3269     </xs:complexType>
3270
3271     <xs:complexType name="AuthenticatorTransportProtocolType">
3272       <xs:complexContent>
3273         <xs:restriction base="AuthenticatorTransportProtocolType">
3274           <xs:sequence>
3275             <xs:choice>
3276               <xs:element ref="PSTN"/>
3277               <xs:element ref="ISDN"/>
3278               <xs:element ref="ADSL"/>
3279             </xs:choice>
3280             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3281           </xs:sequence>
3282         </xs:restriction>
3283       </xs:complexContent>
3284     </xs:complexType>
3285
3286   </xs:redefine>
3287
3288 </xs:schema>

```

3289 **3.4.19 Telephony ("Nomadic")**

3290 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony

3291 Note that this URI is also used as the target namespace in the corresponding authentication context class
3292 schema document ([SAMLAC-TNom]).

3293 Indicates that the principal is "roaming" (perhaps using a phone card) and authenticates via the means of
3294 the line number, a user suffix, and a password element.

```

3295 <?xml version="1.0" encoding="UTF-8"?>
3296
3297 <xs:schema
3298 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3299 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3300 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3301 finalDefault="extension"
3302 blockDefault="substitution"
3303 version="2.0">
3304
3305   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3306
3307     <xs:annotation>

```



```

3308     <xs:documentation>
3309         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
3310         Document identifier: sstc-saml-schema-authn-context-nomad-telephony-2.0
3311         Location: http://www.oasis-
3312 open.org/committees/documents.php?wg_abbrev=security
3313         Revision history:
3314             V2.0 CD-04 (January, 2005):
3315             New authentication context class schema for SAML V2.0.
3316     </xs:documentation>
3317 </xs:annotation>
3318
3319 <xs:complexType name="AuthnContextDeclarationBaseType">
3320     <xs:complexContent>
3321         <xs:restriction base="AuthnContextDeclarationBaseType">
3322             <xs:sequence>
3323                 <xs:element ref="Identification" minOccurs="0"/>
3324                 <xs:element ref="TechnicalProtection" minOccurs="0"/>
3325                 <xs:element ref="OperationalProtection" minOccurs="0"/>
3326                 <xs:element ref="AuthnMethod"/>
3327                 <xs:element ref="GoverningAgreements" minOccurs="0"/>
3328                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3329             </xs:sequence>
3330             <xs:attribute name="ID" type="xs:ID" use="optional"/>
3331         </xs:restriction>
3332     </xs:complexContent>
3333 </xs:complexType>
3334
3335 <xs:complexType name="AuthnMethodBaseType">
3336     <xs:complexContent>
3337         <xs:restriction base="AuthnMethodBaseType">
3338             <xs:sequence>
3339                 <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3340                 <xs:element ref="Authenticator"/>
3341                 <xs:element ref="AuthenticatorTransportProtocol"/>
3342                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3343             </xs:sequence>
3344         </xs:restriction>
3345     </xs:complexContent>
3346 </xs:complexType>
3347
3348 <xs:complexType name="AuthenticatorBaseType">
3349     <xs:complexContent>
3350         <xs:restriction base="AuthenticatorBaseType">
3351             <xs:sequence>
3352                 <xs:element ref="Password"/>
3353                 <xs:element ref="SubscriberLineNumber"/>
3354                 <xs:element ref="UserSuffix"/>
3355             </xs:sequence>
3356         </xs:restriction>
3357     </xs:complexContent>
3358 </xs:complexType>
3359
3360 <xs:complexType name="AuthenticatorTransportProtocolType">
3361     <xs:complexContent>
3362         <xs:restriction base="AuthenticatorTransportProtocolType">
3363             <xs:sequence>
3364                 <xs:choice>
3365                     <xs:element ref="PSTN"/>
3366                     <xs:element ref="ISDN"/>
3367                     <xs:element ref="ADSL"/>
3368                 </xs:choice>
3369                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3370             </xs:sequence>
3371         </xs:restriction>
3372     </xs:complexContent>
3373 </xs:complexType>
3374

```

```
3375     </xs:redefine>
3376
3377 </xs:schema>
```

3378 **3.4.20 Telephony (Personalized)**

3379 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony

3380 Note that this URI is also used as the target namespace in the corresponding authentication context class
3381 schema document ([SAMLAC-TPers]).

3382 This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone
3383 number and a user suffix, transported via a telephony protocol such as ADSL.

```
3384 <?xml version="1.0" encoding="UTF-8"?>
3385
3386 <xs:schema
3387   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
3388   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3389   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
3390   finalDefault="extension"
3391   blockDefault="substitution"
3392   version="2.0">
3393
3394   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3395
3396     <xs:annotation>
3397       <xs:documentation>
3398         Class identifier:
3399 urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony
3400         Document identifier: sstc-saml-schema-authn-context-personal-telephony-
3401 2.0
3402         Location: http://www.oasis-
3403 open.org/committees/documents.php?wg_abbrev=security
3404         Revision history:
3405           V2.0 CD-04 (January, 2005):
3406             New authentication context class schema for SAML V2.0.
3407       </xs:documentation>
3408     </xs:annotation>
3409
3410     <xs:complexType name="AuthnContextDeclarationBaseType">
3411       <xs:complexContent>
3412         <xs:restriction base="AuthnContextDeclarationBaseType">
3413           <xs:sequence>
3414             <xs:element ref="Identification" minOccurs="0"/>
3415             <xs:element ref="TechnicalProtection" minOccurs="0"/>
3416             <xs:element ref="OperationalProtection" minOccurs="0"/>
3417             <xs:element ref="AuthnMethod"/>
3418             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3419             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3420           </xs:sequence>
3421           <xs:attribute name="ID" type="xs:ID" use="optional"/>
3422         </xs:restriction>
3423       </xs:complexContent>
3424     </xs:complexType>
3425
3426     <xs:complexType name="AuthnMethodBaseType">
3427       <xs:complexContent>
3428         <xs:restriction base="AuthnMethodBaseType">
3429           <xs:sequence>
3430             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3431             <xs:element ref="Authenticator"/>
3432             <xs:element ref="AuthenticatorTransportProtocol"/>
3433             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3434           </xs:sequence>
3435         </xs:restriction>
```

```

3436     </xs:complexContent>
3437 </xs:complexType>
3438
3439 <xs:complexType name="AuthenticatorBaseType">
3440 <xs:complexContent>
3441 <xs:restriction base="AuthenticatorBaseType">
3442 <xs:sequence>
3443 <xs:element ref="SubscriberLineNumber"/>
3444 <xs:element ref="UserSuffix"/>
3445 </xs:sequence>
3446 </xs:restriction>
3447 </xs:complexContent>
3448 </xs:complexType>
3449
3450 <xs:complexType name="AuthenticatorTransportProtocolType">
3451 <xs:complexContent>
3452 <xs:restriction base="AuthenticatorTransportProtocolType">
3453 <xs:sequence>
3454 <xs:choice>
3455 <xs:element ref="PSTN"/>
3456 <xs:element ref="ISDN"/>
3457 <xs:element ref="ADSL"/>
3458 </xs:choice>
3459 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3460 </xs:sequence>
3461 </xs:restriction>
3462 </xs:complexContent>
3463 </xs:complexType>
3464
3465 </xs:redefine>
3466
3467 </xs:schema>

```

3468 3.4.21 Telephony (Authenticated)

3469 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony

3470 Note that this URI is also used as the target namespace in the corresponding authentication context class
3471 schema document ([SAMLAC-TAuthn]).

3472 Indicates that the principal authenticated via the means of the line number, a user suffix, and a password
3473 element.

```

3474 <?xml version="1.0" encoding="UTF-8"?>
3475
3476 <xs:schema
3477 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3478 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3479 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3480 finalDefault="extension"
3481 blockDefault="substitution"
3482 version="2.0">
3483
3484 <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3485
3486 <xs:annotation>
3487 <xs:documentation>
3488 Class identifier:
3489 urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
3490 Document identifier: sstc-saml-schema-authn-context-auth-telephony-2.0
3491 Location: http://www.oasis-
3492 open.org/committees/documents.php?wg_abbrev=security
3493 Revision history:
3494 V2.0 CD-04 (January, 2005):
3495 New authentication context class schema for SAML V2.0.
3496 </xs:documentation>

```

```

3497     </xs:annotation>
3498
3499     <xs:complexType name="AuthnContextDeclarationBaseType">
3500       <xs:complexContent>
3501         <xs:restriction base="AuthnContextDeclarationBaseType">
3502           <xs:sequence>
3503             <xs:element ref="Identification" minOccurs="0"/>
3504             <xs:element ref="TechnicalProtection" minOccurs="0"/>
3505             <xs:element ref="OperationalProtection" minOccurs="0"/>
3506             <xs:element ref="AuthnMethod"/>
3507             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3508             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3509           </xs:sequence>
3510           <xs:attribute name="ID" type="xs:ID" use="optional"/>
3511         </xs:restriction>
3512       </xs:complexContent>
3513     </xs:complexType>
3514
3515     <xs:complexType name="AuthnMethodBaseType">
3516       <xs:complexContent>
3517         <xs:restriction base="AuthnMethodBaseType">
3518           <xs:sequence>
3519             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3520             <xs:element ref="Authenticator"/>
3521             <xs:element ref="AuthenticatorTransportProtocol"/>
3522             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3523           </xs:sequence>
3524         </xs:restriction>
3525       </xs:complexContent>
3526     </xs:complexType>
3527
3528     <xs:complexType name="AuthenticatorBaseType">
3529       <xs:complexContent>
3530         <xs:restriction base="AuthenticatorBaseType">
3531           <xs:sequence>
3532             <xs:element ref="Password"/>
3533             <xs:element ref="SubscriberLineNumber"/>
3534             <xs:element ref="UserSuffix"/>
3535           </xs:sequence>
3536         </xs:restriction>
3537       </xs:complexContent>
3538     </xs:complexType>
3539
3540     <xs:complexType name="AuthenticatorTransportProtocolType">
3541       <xs:complexContent>
3542         <xs:restriction base="AuthenticatorTransportProtocolType">
3543           <xs:sequence>
3544             <xs:choice>
3545               <xs:element ref="PSTN"/>
3546               <xs:element ref="ISDN"/>
3547               <xs:element ref="ADSL"/>
3548             </xs:choice>
3549             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3550           </xs:sequence>
3551         </xs:restriction>
3552       </xs:complexContent>
3553     </xs:complexType>
3554   </xs:redefine>
3555 </xs:schema>

```

3557 **3.4.22 Secure Remote Password**

3558 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword

3559 Note that this URI is also used as the target namespace in the corresponding authentication context class

3560 schema document ([SAMLAC-SRP]).

3561 The Secure Remote Password class is applicable when the authentication was performed by means of
3562 Secure Remote Password as specified in [RFC 2945].

```
3563 <?xml version="1.0" encoding="UTF-8"?>
3564
3565 <xs:schema
3566 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
3567 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3568 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
3569 finalDefault="extension"
3570 blockDefault="substitution"
3571 version="2.0">
3572
3573 <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3574
3575 <xs:annotation>
3576 <xs:documentation>
3577 Class identifier:
3578 urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
3579 Document identifier: sstc-saml-schema-authn-context-srp-2.0
3580 Location: http://www.oasis-
3581 open.org/committees/documents.php?wg_abbrev=security
3582 Revision history:
3583 V2.0 CD-04 (January, 2005):
3584 New authentication context class schema for SAML V2.0.
3585 </xs:documentation>
3586 </xs:annotation>
3587
3588 <xs:complexType name="AuthnContextDeclarationBaseType">
3589 <xs:complexContent>
3590 <xs:restriction base="AuthnContextDeclarationBaseType">
3591 <xs:sequence>
3592 <xs:element ref="Identification" minOccurs="0"/>
3593 <xs:element ref="TechnicalProtection" minOccurs="0"/>
3594 <xs:element ref="OperationalProtection" minOccurs="0"/>
3595 <xs:element ref="AuthnMethod"/>
3596 <xs:element ref="GoverningAgreements" minOccurs="0"/>
3597 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3598 </xs:sequence>
3599 <xs:attribute name="ID" type="xs:ID" use="optional"/>
3600 </xs:restriction>
3601 </xs:complexContent>
3602 </xs:complexType>
3603
3604 <xs:complexType name="AuthnMethodBaseType">
3605 <xs:complexContent>
3606 <xs:restriction base="AuthnMethodBaseType">
3607 <xs:sequence>
3608 <xs:element ref="PrincipalAuthenticationMechanism"/>
3609 <xs:element ref="Authenticator"/>
3610 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
3611 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3612 </xs:sequence>
3613 </xs:restriction>
3614 </xs:complexContent>
3615 </xs:complexType>
3616
3617 <xs:complexType name="PrincipalAuthenticationMechanismType">
3618 <xs:complexContent>
3619 <xs:restriction base="PrincipalAuthenticationMechanismType">
3620 <xs:sequence>
3621 <xs:element ref="RestrictedPassword"/>
3622 </xs:sequence>
3623 </xs:restriction>
3624 </xs:complexContent>
3625 </xs:complexType>
```

```

3626
3627     <xs:complexType name="AuthenticatorBaseType">
3628     <xs:complexContent>
3629     <xs:restriction base="AuthenticatorBaseType">
3630     <xs:sequence>
3631     <xs:element ref="SharedSecretChallengeResponse"/>
3632     </xs:sequence>
3633     </xs:restriction>
3634     </xs:complexContent>
3635     </xs:complexType>
3636
3637     <xs:complexType name="SharedSecretChallengeResponseType">
3638     <xs:complexContent>
3639     <xs:restriction base="SharedSecretChallengeResponseType">
3640     <xs:attribute name="method" type="xs:anyURI"
3641     fixed="urn:ietf:rfc:2945"/>
3642     </xs:restriction>
3643     </xs:complexContent>
3644     </xs:complexType>
3645
3646     </xs:redefine>
3647
3648 </xs:schema>

```

3649 **3.4.23 SSL/TLS Certificate-Based Client Authentication**

3650 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TLSCClient

3651 Note that this URI is also used as the target namespace in the corresponding authentication context class
3652 schema document ([SAMLAC-SSL]).

3653 This class indicates that the principal authenticated by means of a client certificate, secured with the
3654 SSL/TLS transport.

```

3655 <?xml version="1.0" encoding="UTF-8"?>
3656
3657 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSCClient"
3658   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3659   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSCClient"
3660   finalDefault="extension"
3661   blockDefault="substitution"
3662   version="2.0">
3663
3664   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3665
3666     <xs:annotation>
3667     <xs:documentation>
3668     Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TLSCClient
3669     Document identifier: sstc-saml-schema-authn-context-sslcert-2.0
3670     Location: http://www.oasis-
3671     open.org/committees/documents.php?wg_abbrev=security
3672     Revision history:
3673     V2.0 CD-04 (January, 2005):
3674     New authentication context class schema for SAML V2.0.
3675     </xs:documentation>
3676     </xs:annotation>
3677
3678     <xs:complexType name="AuthnContextDeclarationBaseType">
3679     <xs:complexContent>
3680     <xs:restriction base="AuthnContextDeclarationBaseType">
3681     <xs:sequence>
3682     <xs:element ref="Identification" minOccurs="0"/>
3683     <xs:element ref="TechnicalProtection" minOccurs="0"/>
3684     <xs:element ref="OperationalProtection" minOccurs="0"/>
3685     <xs:element ref="AuthnMethod"/>
3686     <xs:element ref="GoverningAgreements" minOccurs="0"/>

```

```

3687         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3688     </xs:sequence>
3689     <xs:attribute name="ID" type="xs:ID" use="optional"/>
3690 </xs:restriction>
3691 </xs:complexContent>
3692 </xs:complexType>
3693
3694 <xs:complexType name="AuthnMethodBaseType">
3695     <xs:complexContent>
3696         <xs:restriction base="AuthnMethodBaseType">
3697             <xs:sequence>
3698                 <xs:element ref="PrincipalAuthenticationMechanism"/>
3699                 <xs:element ref="Authenticator"/>
3700                 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
3701                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3702             </xs:sequence>
3703         </xs:restriction>
3704     </xs:complexContent>
3705 </xs:complexType>
3706
3707 <xs:complexType name="PrincipalAuthenticationMechanismType">
3708     <xs:complexContent>
3709         <xs:restriction base="PrincipalAuthenticationMechanismType">
3710             <xs:sequence>
3711                 <xs:element ref="RestrictedPassword"/>
3712             </xs:sequence>
3713             <xs:attribute name="preauth" type="xs:integer" use="optional"/>
3714         </xs:restriction>
3715     </xs:complexContent>
3716 </xs:complexType>
3717
3718 <xs:complexType name="AuthenticatorBaseType">
3719     <xs:complexContent>
3720         <xs:restriction base="AuthenticatorBaseType">
3721             <xs:sequence>
3722                 <xs:element ref="DigSig"/>
3723             </xs:sequence>
3724         </xs:restriction>
3725     </xs:complexContent>
3726 </xs:complexType>
3727
3728 <xs:complexType name="PublicKeyType">
3729     <xs:complexContent>
3730         <xs:restriction base="PublicKeyType">
3731             <xs:attribute name="keyValidation" type="xs:anyURI"
3732 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
3733         </xs:restriction>
3734     </xs:complexContent>
3735 </xs:complexType>
3736
3737 <xs:complexType name="AuthenticatorTransportProtocolType">
3738     <xs:complexContent>
3739         <xs:restriction base="AuthenticatorTransportProtocolType">
3740             <xs:sequence>
3741                 <xs:choice>
3742                     <xs:element ref="SSL"/>
3743                     <xs:element ref="WTLS"/>
3744                 </xs:choice>
3745                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3746             </xs:sequence>
3747         </xs:restriction>
3748     </xs:complexContent>
3749 </xs:complexType>
3750
3751 </xs:redefine>
3752
3753 </xs:schema>

```

3754 3.4.24 TimeSyncToken

3755 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken

3756 Note that this URI is also used as the target namespace in the corresponding authentication context class
3757 schema document ([SAMLAC-TSTJ]).

3758 The TimeSyncToken class is applicable when a principal authenticates through a time synchronization
3759 token.

```
3760 <?xml version="1.0" encoding="UTF-8"?>
3761
3762 <xs:schema
3763 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
3764 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3765 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
3766 finalDefault="extension"
3767 blockDefault="substitution"
3768 version="2.0">
3769
3770 <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3771
3772 <xs:annotation>
3773 <xs:documentation>
3774 Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
3775 Document identifier: sstc-saml-schema-authn-context-timesync-2.0
3776 Location: http://www.oasis-
3777 open.org/committees/documents.php?wg_abbrev=security
3778 Revision history:
3779 V2.0 CD-04 (January, 2005):
3780 New authentication context class schema for SAML V2.0.
3781 </xs:documentation>
3782 </xs:annotation>
3783
3784 <xs:complexType name="AuthnContextDeclarationBaseType">
3785 <xs:complexContent>
3786 <xs:restriction base="AuthnContextDeclarationBaseType">
3787 <xs:sequence>
3788 <xs:element ref="Identification" minOccurs="0"/>
3789 <xs:element ref="TechnicalProtection" minOccurs="0"/>
3790 <xs:element ref="OperationalProtection" minOccurs="0"/>
3791 <xs:element ref="AuthnMethod"/>
3792 <xs:element ref="GoverningAgreements" minOccurs="0"/>
3793 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3794 </xs:sequence>
3795 <xs:attribute name="ID" type="xs:ID" use="optional"/>
3796 </xs:restriction>
3797 </xs:complexContent>
3798 </xs:complexType>
3799
3800 <xs:complexType name="AuthnMethodBaseType">
3801 <xs:complexContent>
3802 <xs:restriction base="AuthnMethodBaseType">
3803 <xs:sequence>
3804 <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3805 <xs:element ref="Authenticator"/>
3806 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
3807 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3808 </xs:sequence>
3809 </xs:restriction>
3810 </xs:complexContent>
3811 </xs:complexType>
3812
3813 <xs:complexType name="PrincipalAuthenticationMechanismType">
3814 <xs:complexContent>
3815 <xs:restriction base="PrincipalAuthenticationMechanismType">
```



```

3816     <xs:sequence>
3817         <xs:element ref="Token" />
3818     </xs:sequence>
3819 </xs:restriction>
3820 </xs:complexContent>
3821 </xs:complexType>
3822
3823 <xs:complexType name="TokenType">
3824     <xs:complexContent>
3825         <xs:restriction base="TokenType">
3826             <xs:sequence>
3827                 <xs:element ref="TimeSyncToken" />
3828                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
3829             </xs:sequence>
3830         </xs:restriction>
3831     </xs:complexContent>
3832 </xs:complexType>
3833
3834 <xs:complexType name="TimeSyncTokenType">
3835     <xs:complexContent>
3836         <xs:restriction base="TimeSyncTokenType">
3837             <xs:attribute name="DeviceType" use="required">
3838                 <xs:simpleType>
3839                     <xs:restriction base="DeviceTypeType">
3840                         <xs:enumeration value="hardware" />
3841                     </xs:restriction>
3842                 </xs:simpleType>
3843             </xs:attribute>
3844
3845             <xs:attribute name="SeedLength" use="required">
3846                 <xs:simpleType>
3847                     <xs:restriction base="xs:integer">
3848                         <xs:minInclusive value="64" />
3849                     </xs:restriction>
3850                 </xs:simpleType>
3851             </xs:attribute>
3852
3853             <xs:attribute name="DeviceInHand" use="required">
3854                 <xs:simpleType>
3855                     <xs:restriction base="booleanType">
3856                         <xs:enumeration value="true" />
3857                     </xs:restriction>
3858                 </xs:simpleType>
3859             </xs:attribute>
3860         </xs:restriction>
3861     </xs:complexContent>
3862 </xs:complexType>
3863
3864 </xs:redefine>
3865
3866 </xs:schema>

```

3867 **3.4.25 Unspecified**

3868 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

3869 The Unspecified class indicates that the authentication was performed by unspecified means.

4 References

3870

- 3871 [RFC 1510] J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5)*. IETF
3872 RFC 1510, September 1993. <http://www.ietf.org/rfc/rfc1510.txt>.
- 3873 [RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
3874 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 3875 [RFC 2945] T. Wu. *The SRP Authentication and Key Exchange System*. IETF RFC 2945,
3876 September 2000. <http://www.ietf.org/rfc/rfc2945.txt>.
- 3877 [SAMLAC-xsd] J. Kemp et al., SAML authentication context schema. OASIS SSTC, January
3878 2005. Document ID sstc-saml-schema-authn-context-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
3879 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 3880 [SAMLAC-Types] J. Kemp et al., SAML authentication context types schema. OASIS SSTC,
3881 January 2005. Document ID sstc-saml-schema-authn-context-types-2.0. See
3882 <http://www.oasis-open.org/committees/security/>.
- 3883 [SAMLAC-IP] J. Kemp et al., SAML context class schema for Internet Protocol. OASIS SSTC,
3884 January 2005. Document ID sstc-saml-schema-authn-context-ip-2.0. See
3885 <http://www.oasis-open.org/committees/security/>.
- 3886 [SAMLAC-IPP] J. Kemp et al., SAML context class schema for Internet Protocol Password.
3887 OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-
3888 <http://www.oasis-open.org/committees/security/>.
- 3889 [SAMLAC-Kerb] J. Kemp et al., SAML context class schema for Kerberos. OASIS SSTC, January
3890 2005. Document ID sstc-saml-schema-authn-context-kerberos-2.0. See
3891 <http://www.oasis-open.org/committees/security/>.
- 3892 [SAMLAC-MOFC] J. Kemp et al., SAML context class schema for Mobile One Factor Contract.
3893 Document ID sstc-saml-schema-authn-context-mobileonefactor-reg-2.0. See
3894 OASIS SSTC, January 2005. <http://www.oasis-open.org/committees/security/>.
- 3895 [SAMLAC-MOFU] J. Kemp et al., SAML context class schema for Mobile One Factor Unregistered.
3896 Document ID sstc-saml-schema-authn-context-mobileonefactor-unreg-2.0. See
3897 OASIS SSTC, January 2005. <http://www.oasis-open.org/committees/security/>.
- 3898 [SAMLAC-MTFC] J. Kemp et al., SAML context class schema for Mobile Two Factor Contract.
3899 OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-
3900 <http://www.oasis-open.org/committees/security/>.
- 3901 [SAMLAC-MTFU] J. Kemp et al., SAML context class schema for Mobile Two Factor Unregistered.
3902 OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-
3903 <http://www.oasis-open.org/committees/security/>.
- 3904 [SAMLAC-Pass] J. Kemp et al., SAML context class schema for Password. OASIS SSTC, January
3905 2005. Document ID sstc-saml-schema-authn-context-pword-2.0. See
3906 <http://www.oasis-open.org/committees/security/>.
- 3907 [SAMLAC-PGP] J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC,
3908 January 2005. Document ID sstc-saml-schema-authn-context-pgp-2.0. See
3909 <http://www.oasis-open.org/committees/security/>.
- 3910 [SAMLAC-PPT] J. Kemp et al., SAML context class schema for Password Protected Transport.
3911 OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-ppt-
3912 <http://www.oasis-open.org/committees/security/>.
- 3913 [SAMLAC-Prev] J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC,
3914 January 2005. Document ID sstc-saml-schema-authn-context-session-2.0. See
3915 <http://www.oasis-open.org/committees/security/>.
- 3916 [SAMLAC-Smart] J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC,
3917 January 2005. Document ID sstc-saml-schema-authn-context-smartcard-2.0. See

3918 <http://www.oasis-open.org/committees/security/>.

3919 **[SAMLAC-SmPKI]** J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC,
3920 January 2005. Document ID sstc-saml-schema-authn-context-smartcardpki-2.0.
3921 See <http://www.oasis-open.org/committees/security/>.

3922 **[SAMLAC-SPKI]** J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC,
3923 January 2005. Document ID sstc-saml-schema-authn-context-spmki-2.0. See
3924 <http://www.oasis-open.org/committees/security/>.

3925 **[SAMLAC-SRP]** J. Kemp et al., SAML context class schema for Secure Remote Password.
3926 OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-srp-
3927 2.0. See <http://www.oasis-open.org/committees/security/>.

3928 **[SAMLAC-SSL]** J. Kemp et al., SAML context class schema for SSL/TLS Certificate-Based Client
3929 Authentication. OASIS SSTC, January 2005. Document ID sstc-saml-schema-
3930 authn-context-sslcert-2.0. See <http://www.oasis-open.org/committees/security/>.

3931 **[SAMLAC-SwPKI]** J. Kemp et al., SAML context class schema for Software PKI. OASIS SSTC,
3932 January 2005. Document ID sstc-saml-schema-authn-context-softwarepki-2.0.
3933 See <http://www.oasis-open.org/committees/security/>.

3934 **[SAMLAC-Tele]** J. Kemp et al., SAML context class schema for Telephony. OASIS SSTC,
3935 January 2005. Document ID sstc-saml-schema-authn-context-telephony-2.0. See
3936 <http://www.oasis-open.org/committees/security/>.

3937 **[SAMLAC-TNom]** J. Kemp et al., SAML context class schema for Telephony (“Nomadic”). OASIS
3938 SSTC, January 2005. Document ID sstc-saml-schema-authn-context-nomad-
3939 telephony-2.0. See <http://www.oasis-open.org/committees/security/>.

3940 **[SAMLAC-TPers]** J. Kemp et al., SAML context class schema for Telephony (Personalized). OASIS
3941 SSTC, January 2005. Document ID sstc-saml-schema-authn-context-personal-
3942 telephony-2.0. See <http://www.oasis-open.org/committees/security/>.

3943 **[SAMLAC-TAuthn]** J. Kemp et al., SAML context class schema for Telephony (Authenticated).
3944 OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-
3945 auth-telephony-2.0. See <http://www.oasis-open.org/committees/security/>.

3946 **[SAMLAC-TST]** J. Kemp et al., SAML context class schema for Time Sync Token. OASIS SSTC,
3947 January 2005. Document ID sstc-saml-schema-authn-context-timesync-2.0. See
3948 <http://www.oasis-open.org/committees/security/>.

3949 **[SAMLAC-X509]** J. Kemp et al., SAML context class schema for Public Key – X.509. OASIS
3950 SSTC, January 2005. Document ID sstc-saml-schema-authn-context-x509-2.0.
3951 See <http://www.oasis-open.org/committees/security/>.

3952 **[SAMLAC-XSig]** J. Kemp et al., SAML context class schema for Public Key – XML Signature.
3953 OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-
3954 xmldsig-2.0. See <http://www.oasis-open.org/committees/security/>.

3955 **[SAMLCore]** S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion
3956 Markup Language (SAML) V2.0*. OASIS SSTC, January 2005. Document ID sstc-
3957 saml-core-2.0-cd-04. See <http://www.oasis-open.org/committees/security/>.

3958 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
3959 Consortium Recommendation, May 2001. <http://www.w3.org/TR/xmlschema-1/>.

3960 **[XMLSig]** D. Eastlake et al., *XML-Signature Syntax and Processing*, World Wide Web
3961 Consortium, February 2002. <http://www.w3.org/TR/xmldsig-core/>.

3962 Appendix A. Acknowledgments

3963 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
3964 Committee, whose voting members at the time of publication were:

- 3965 • Conor Cahill, AOL
- 3966 • John Hughes, Atos Origin
- 3967 • Hal Lockhart, BEA Systems
- 3968 • Mike Beach, Boeing
- 3969 • Rebekah Metz, Booz Allen Hamilton
- 3970 • Rick Randall, Booz Allen Hamilton
- 3971 • Ronald Jacobson, Computer Associates
- 3972 • Carolina Canales-Valenzuela, Ericsson
- 3973 • Dana Kaufman, Forum Systems
- 3974 • Irving Reid, Hewlett-Packard
- 3975 • Paula Austel, IBM
- 3976 • Michael McIntosh, IBM
- 3977 • Anthony Nadalin, IBM
- 3978 • Nick Ragouzis, Individual
- 3979 • Scott Cantor, Internet2
- 3980 • Bob Morgan, Internet2
- 3981 • Peter Davis, Neustar
- 3982 • Jeff Hodges, Neustar
- 3983 • Frederick Hirsch, Nokia
- 3984 • Senthil Sengodan, Nokia
- 3985 • Abbie Barbir, Nortel Networks
- 3986 • Scott Kiestler, Novell
- 3987 • Cameron Morris, Novell
- 3988 • Paul Madsen, NTT
- 3989 • Steve Anderson, OpenNetwork
- 3990 • Ari Kermaier, Oracle
- 3991 • Vamsi Motukuru, Oracle
- 3992 • Darren Platt, Ping Identity
- 3993 • Prateek Mishra, Principal Identity
- 3994 • Jim Lien, RSA Security
- 3995 • John Linn, RSA Security
- 3996 • Rob Philpott, RSA Security
- 3997 • Dipak Chopra, SAP
- 3998 • Jahan Moreh, Sigaba
- 3999 • Bhavna Bhatnagar, Sun Microsystems
- 4000 • Eve Maler, Sun Microsystems
- 4001 • Ronald Monzillo, Sun Microsystems
- 4002 • Emily Xu, Sun Microsystems
- 4003 • Greg Whitehead, Trustgenix
- 4004

4005

4006 The editors also would like to acknowledge the following people for their contributions to previous versions
4007 of the OASIS Security Assertions Markup Language Standard:

- 4008 • Stephen Farrell, Baltimore Technologies
- 4009 • David Orchard, BEA Systems
- 4010 • Krishna Sankar, Cisco Systems
- 4011 • Zahid Ahmed, CommerceOne
- 4012 • Carlisle Adams, Entrust
- 4013 • Tim Moses, Entrust
- 4014 • Nigel Edwards, Hewlett-Packard
- 4015 • Joe Pato, Hewlett-Packard
- 4016 • Bob Blakley, IBM
- 4017 • Marlena Erdos, IBM
- 4018 • Marc Chanliau, Netegrity
- 4019 • Chris McLaren, Netegrity
- 4020 • Lynne Rosenthal, NIST
- 4021 • Mark Skall, NIST
- 4022 • Simon Godik, Overxeer
- 4023 • Charles Norwood, SAIC
- 4024 • Evan Prodromou, Securant
- 4025 • Robert Griffin, RSA Security (former editor)
- 4026 • Sai Allarvarpu, Sun Microsystems
- 4027 • Chris Ferris, Sun Microsystems
- 4028 • Mike Myers, Traceroute Security
- 4029 • Phillip Hallam-Baker, VeriSign (former editor)
- 4030 • James Vanderbeek, Vodafone
- 4031 • Mark O'Neill, Vordel
- 4032 • Tony Palmer, Vordel

4033

4034 Finally, the editors wish to acknowledge the following people for their contributions of material used as
4035 input to the OASIS Security Assertions Markup Language specifications:

- 4036 • Thomas Gross, IBM
- 4037 • Birgit Pfitzmann, IBM

4038 Appendix B. Notices

4039 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
4040 might be claimed to pertain to the implementation or use of the technology described in this document or
4041 the extent to which any license under such rights might or might not be available; neither does it represent
4042 that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to
4043 rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made
4044 available for publication and any assurances of licenses to be made available, or the result of an attempt
4045 made to obtain a general license or permission for the use of such proprietary rights by implementors or
4046 users of this specification, can be obtained from the OASIS Executive Director.

4047 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or
4048 other proprietary rights which may cover technology that may be required to implement this specification.
4049 Please address the information to the OASIS Executive Director.

4050 **Copyright © OASIS Open 2005. All Rights Reserved.**

4051 This document and translations of it may be copied and furnished to others, and derivative works that
4052 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and
4053 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
4054 this paragraph are included on all such copies and derivative works. However, this document itself does
4055 not be modified in any way, such as by removing the copyright notice or references to OASIS, except as
4056 needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights
4057 defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it
4058 into languages other than English.

4059 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
4060 or assigns.

4061 This document and the information contained herein is provided on an "AS IS" basis and OASIS
4062 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
4063 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR
4064 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.