



1

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

5 OASIS Standard, 15 March 2005

6 **Document identifier:**

7 saml-authn-context-2.0-os

8 **Location:**

9 <http://docs.oasis-open.org/security/saml/v2.0/>

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 Thomas Wisniewski, Entrust
24 Irving Reid, Hewlett-Packard
25 Paula Austel, IBM
26 Maryann Hondo, IBM
27 Michael McIntosh, IBM
28 Tony Nadalin, IBM
29 Nick Ragouzis, Individual
30 Scott Cantor, Internet2
31 RL 'Bob' Morgan, Internet2
32 Peter C Davis, Neustar
33 Jeff Hodges, Neustar
34 Frederick Hirsch, Nokia
35 John Kemp, Nokia
36 Paul Madsen, NTT
37 Steve Anderson, OpenNetwork
38 Prateek Mishra, Principal Identity
39 John Linn, RSA Security
40 Rob Philpott, RSA Security
41 Jahan Moreh, Sigaba
42 Anne Anderson, Sun Microsystems
43 Eve Maler, Sun Microsystems
44 Ron Monzillo, Sun Microsystems

45 Greg Whitehead, Trustgenix

46 **Abstract:**

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

49 **Status:**

50 This is an **OASIS Standard** document produced by the Security Services Technical Committee. It
51 was approved by the OASIS membership on 1 March 2005.

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

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

61 Table of Contents

62	1 Introduction.....	4
63	1.1 Authentication Context Concepts.....	4
64	1.2 Notation and Terminology.....	4
65	2 Authentication Context Declaration.....	6
66	2.1 Data Model.....	6
67	2.2 Extensibility.....	7
68	2.3 Processing Rules.....	7
69	2.4 Schema.....	7
70	3 Authentication Context Classes.....	21
71	3.1 Advantages of Authentication Context Classes.....	21
72	3.2 Processing Rules.....	21
73	3.3 Extensibility.....	22
74	3.4 Schemas.....	22
75	3.4.1 Internet Protocol.....	22
76	3.4.2 InternetProtocolPassword.....	24
77	3.4.3 Kerberos.....	25
78	3.4.4 MobileOneFactorUnregistered.....	27
79	3.4.5 MobileTwoFactorUnregistered.....	30
80	3.4.6 MobileOneFactorContract.....	33
81	3.4.7 MobileTwoFactorContract.....	36
82	3.4.8 Password.....	39
83	3.4.9 PasswordProtectedTransport.....	41
84	3.4.10 PreviousSession.....	42
85	3.4.11 Public Key – X.509.....	44
86	3.4.12 Public Key – PGP.....	45
87	3.4.13 Public Key – SPKI.....	46
88	3.4.14 Public Key - XML Digital Signature.....	48
89	3.4.15 Smartcard.....	49
90	3.4.16 SmartcardPKI.....	50
91	3.4.17 SoftwarePKI.....	53
92	3.4.18 Telephony.....	55
93	3.4.19 Telephony ("Nomadic").....	56
94	3.4.20 Telephony (Personalized).....	57
95	3.4.21 Telephony (Authenticated).....	59
96	3.4.22 Secure Remote Password.....	60
97	3.4.23 SSL/TLS Certificate-Based Client Authentication.....	62
98	3.4.24 TimeSyncToken.....	63
99	3.4.25 Unspecified.....	65
100	4 References.....	66
101	Appendix A. Acknowledgments.....	68
102	Appendix B. Notices.....	70
103		

1 Introduction

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

1.1 Authentication Context Concepts

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

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

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

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

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

1.2 Notation and Terminology

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

139 `Listings of XML schemas appear like this.`

140 `Example code listings appear like this.`

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

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

149 their respective namespaces as follows, whether or not a namespace declaration is present in the
150 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].

151

152 This specification uses the following typographical conventions in text: <SAML**E**lement>,
153 <ns:ForeignElement>, XMLAttribute, **Datatype**, OtherKeyword.

2 Authentication Context Declaration

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

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

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

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

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

2.1 Data Model

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

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

194 2.2 Extensibility

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

201 2.3 Processing Rules

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

207 2.4 Schema

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

```
211 <?xml version="1.0" encoding="UTF-8"?>
212 <xs:schema
213   xmlns:xs="http://www.w3.org/2001/XMLSchema"
214   elementFormDefault="qualified"
215   version="2.0">
216
217   <xs:annotation>
218     <xs:documentation>
219       Document identifier: saml-schema-authn-context-types-2.0
220       Location: http://docs.oasis-open.org/security/saml/v2.0/
221       Revision history:
222         V2.0 (March, 2005):
223         New core authentication context schema types for SAML V2.0.
224     </xs:documentation>
225   </xs:annotation>
226
227   <xs:element name="AuthenticationContextDeclaration"
228     type="AuthnContextDeclarationBaseType">
229     <xs:annotation>
230       <xs:documentation>
231         A particular assertion on an identity
232         provider's part with respect to the authentication
233         context associated with an authentication assertion.
234       </xs:documentation>
235     </xs:annotation>
236   </xs:element>
237
238   <xs:element name="Identification" type="IdentificationType">
239     <xs:annotation>
240       <xs:documentation>
241         Refers to those characteristics that describe the
242         processes and mechanisms
243         the Authentication Authority uses to initially create
244         an association between a Principal
245         and the identity (or name) by which the Principal will
246         be known
247       </xs:documentation>
248     </xs:annotation>
249   </xs:element>
```

```

250
251 <xs:element name="PhysicalVerification">
252   <xs:annotation>
253     <xs:documentation>
254       This element indicates that identification has been
255       performed in a physical
256       face-to-face meeting with the principal and not in an
257       online manner.
258     </xs:documentation>
259   </xs:annotation>
260   <xs:complexType>
261     <xs:attribute name="credentialLevel">
262       <xs:simpleType>
263         <xs:restriction base="xs:NMTOKEN">
264           <xs:enumeration value="primary"/>
265           <xs:enumeration value="secondary"/>
266         </xs:restriction>
267       </xs:simpleType>
268     </xs:attribute>
269   </xs:complexType>
270 </xs:element>
271
272 <xs:element name="WrittenConsent" type="ExtensionOnlyType"/>
273
274 <xs:element name="TechnicalProtection" type="TechnicalProtectionBaseType">
275   <xs:annotation>
276     <xs:documentation>
277       Refers to those characteristics that describe how the
278       'secret' (the knowledge or possession
279       of which allows the Principal to authenticate to the
280       Authentication Authority) is kept secure
281     </xs:documentation>
282   </xs:annotation>
283 </xs:element>
284
285 <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType">
286   <xs:annotation>
287     <xs:documentation>
288       This element indicates the types and strengths of
289       facilities
290       of a UA used to protect a shared secret key from
291       unauthorized access and/or use.
292     </xs:documentation>
293   </xs:annotation>
294 </xs:element>
295
296 <xs:element name="PrivateKeyProtection" type="PrivateKeyProtectionType">
297   <xs:annotation>
298     <xs:documentation>
299       This element indicates the types and strengths of
300       facilities
301       of a UA used to protect a private key from
302       unauthorized access and/or use.
303     </xs:documentation>
304   </xs:annotation>
305 </xs:element>
306
307 <xs:element name="KeyActivation" type="KeyActivationType">
308   <xs:annotation>
309     <xs:documentation>The actions that must be performed
310     before the private key can be used. </xs:documentation>
311   </xs:annotation>
312 </xs:element>
313
314 <xs:element name="KeySharing" type="KeySharingType">
315   <xs:annotation>
316     <xs:documentation>Whether or not the private key is shared

```



```

317         with the certificate authority.</xs:documentation>
318     </xs:annotation>
319 </xs:element>
320
321 <xs:element name="KeyStorage" type="KeyStorageType">
322     <xs:annotation>
323         <xs:documentation>
324             In which medium is the key stored.
325             memory - the key is stored in memory.
326             smartcard - the key is stored in a smartcard.
327             token - the key is stored in a hardware token.
328             MobileDevice - the key is stored in a mobile device.
329             MobileAuthCard - the key is stored in a mobile
330             authentication card.
331         </xs:documentation>
332     </xs:annotation>
333 </xs:element>
334
335 <xs:element name="SubscriberLineNumber" type="ExtensionOnlyType"/>
336 <xs:element name="UserSuffix" type="ExtensionOnlyType"/>
337
338 <xs:element name="Password" type="PasswordType">
339     <xs:annotation>
340         <xs:documentation>
341             This element indicates that a password (or passphrase)
342             has been used to
343             authenticate the Principal to a remote system.
344         </xs:documentation>
345     </xs:annotation>
346 </xs:element>
347
348 <xs:element name="ActivationPin" type="ActivationPinType">
349     <xs:annotation>
350         <xs:documentation>
351             This element indicates that a Pin (Personal
352             Identification Number) has been used to authenticate the Principal to
353             some local system in order to activate a key.
354         </xs:documentation>
355     </xs:annotation>
356 </xs:element>
357
358 <xs:element name="Token" type="TokenType">
359     <xs:annotation>
360         <xs:documentation>
361             This element indicates that a hardware or software
362             token is used
363             as a method of identifying the Principal.
364         </xs:documentation>
365     </xs:annotation>
366 </xs:element>
367
368 <xs:element name="TimeSyncToken" type="TimeSyncTokenType">
369     <xs:annotation>
370         <xs:documentation>
371             This element indicates that a time synchronization
372             token is used to identify the Principal. hardware -
373             the time synchronization
374             token has been implemented in hardware. software - the
375             time synchronization
376             token has been implemented in software. SeedLength -
377             the length, in bits, of the
378             random seed used in the time synchronization token.
379         </xs:documentation>
380     </xs:annotation>
381 </xs:element>
382
383 <xs:element name="Smartcard" type="ExtensionOnlyType">

```

```

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

```

```

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

```

```

518
519 <xs:complexType name="SharedSecretChallengeResponseType">
520   <xs:annotation>
521     <xs:documentation>
522       This element indicates that the Principal has been
523       authenticated by a challenge-response protocol utilizing shared secret
524       keys and symmetric cryptography.
525     </xs:documentation>
526   </xs:annotation>
527   <xs:sequence>
528     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
529   </xs:sequence>
530   <xs:attribute name="method" type="xs:anyURI" use="optional"/>
531 </xs:complexType>
532
533 <xs:element name="DigSig" type="PublicKeyType">
534   <xs:annotation>
535     <xs:documentation>
536       This element indicates that the Principal has been
537       authenticated by a mechanism which involves the Principal computing a
538       digital signature over at least challenge data provided by the IdP.
539     </xs:documentation>
540   </xs:annotation>
541 </xs:element>
542
543 <xs:element name="AsymmetricDecryption" type="PublicKeyType">
544   <xs:annotation>
545     <xs:documentation>
546       The local system has a private key but it is used
547       in decryption mode, rather than signature mode. For example, the
548       Authentication Authority generates a secret and encrypts it using the
549       local system's public key: the local system then proves it has
550       decrypted the secret.
551     </xs:documentation>
552   </xs:annotation>
553 </xs:element>
554
555 <xs:element name="AsymmetricKeyAgreement" type="PublicKeyType">
556   <xs:annotation>
557     <xs:documentation>
558       The local system has a private key and uses it for
559       shared secret key agreement with the Authentication Authority (e.g.
560       via Diffie Helman).
561     </xs:documentation>
562   </xs:annotation>
563 </xs:element>
564
565 <xs:complexType name="PublicKeyType">
566   <xs:sequence>
567     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
568   </xs:sequence>
569   <xs:attribute name="keyValidation" use="optional"/>
570 </xs:complexType>
571
572 <xs:element name="IPAddress" type="ExtensionOnlyType">
573   <xs:annotation>
574     <xs:documentation>
575       This element indicates that the Principal has been
576       authenticated through connection from a particular IP address.
577     </xs:documentation>
578   </xs:annotation>
579 </xs:element>
580
581 <xs:element name="SharedSecretDynamicPlaintext" type="ExtensionOnlyType">
582   <xs:annotation>
583     <xs:documentation>
584       The local system and Authentication Authority

```

```

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

```

```

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

```

```

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

```

```

786
787 <xs:group name="AuthenticatorSequenceGroup">
788   <xs:sequence>
789     <xs:element ref="PreviousSession" minOccurs="0"/>
790     <xs:element ref="ResumeSession" minOccurs="0"/>
791     <xs:element ref="DigSig" minOccurs="0"/>
792     <xs:element ref="Password" minOccurs="0"/>
793     <xs:element ref="RestrictedPassword" minOccurs="0"/>
794     <xs:element ref="ZeroKnowledge" minOccurs="0"/>
795     <xs:element ref="SharedSecretChallengeResponse" minOccurs="0"/>
796     <xs:element ref="SharedSecretDynamicPlaintext" minOccurs="0"/>
797     <xs:element ref="IPAddress" minOccurs="0"/>
798     <xs:element ref="AsymmetricDecryption" minOccurs="0"/>
799     <xs:element ref="AsymmetricKeyAgreement" minOccurs="0"/>
800     <xs:element ref="SubscriberLineNumber" minOccurs="0"/>
801     <xs:element ref="UserSuffix" minOccurs="0"/>
802     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
803   </xs:sequence>
804 </xs:group>
805
806 <xs:complexType name="AuthenticatorBaseType">
807   <xs:sequence>
808     <xs:group ref="AuthenticatorChoiceGroup"/>
809     <xs:group ref="AuthenticatorSequenceGroup"/>
810   </xs:sequence>
811 </xs:complexType>
812
813 <xs:complexType name="ComplexAuthenticatorType">
814   <xs:sequence>
815     <xs:group ref="AuthenticatorChoiceGroup"/>
816     <xs:group ref="AuthenticatorSequenceGroup"/>
817   </xs:sequence>
818 </xs:complexType>
819
820 <xs:complexType name="AuthenticatorTransportProtocolType">
821   <xs:sequence>
822     <xs:choice minOccurs="0">
823       <xs:element ref="HTTP"/>
824       <xs:element ref="SSL"/>
825       <xs:element ref="MobileNetworkNoEncryption"/>
826       <xs:element ref="MobileNetworkRadioEncryption"/>
827       <xs:element ref="MobileNetworkEndToEndEncryption"/>
828       <xs:element ref="WTLS"/>
829       <xs:element ref="IPSec"/>
830       <xs:element ref="PSTN"/>
831       <xs:element ref="ISDN"/>
832       <xs:element ref="ADSL"/>
833     </xs:choice>
834     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
835   </xs:sequence>
836 </xs:complexType>
837
838 <xs:complexType name="KeyActivationType">
839   <xs:sequence>
840     <xs:element ref="ActivationPin" minOccurs="0"/>
841     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
842   </xs:sequence>
843 </xs:complexType>
844
845 <xs:complexType name="KeySharingType">
846   <xs:attribute name="sharing" type="xs:boolean" use="required"/>
847 </xs:complexType>
848
849 <xs:complexType name="PrivateKeyProtectionType">
850   <xs:sequence>
851     <xs:element ref="KeyActivation" minOccurs="0"/>
852     <xs:element ref="KeyStorage" minOccurs="0"/>

```



```

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

```

```

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

```

```

987
988 <xs:complexType name="LengthType">
989   <xs:attribute name="min" type="xs:integer" use="required"/>
990   <xs:attribute name="max" type="xs:integer" use="optional"/>
991 </xs:complexType>
992
993 <xs:simpleType name="mediumType">
994   <xs:restriction base="xs:NMTOKEN">
995     <xs:enumeration value="memory"/>
996     <xs:enumeration value="smartcard"/>
997     <xs:enumeration value="token"/>
998     <xs:enumeration value="MobileDevice"/>
999     <xs:enumeration value="MobileAuthCard"/>
1000   </xs:restriction>
1001 </xs:simpleType>
1002
1003 <xs:complexType name="KeyStorageType">
1004   <xs:attribute name="medium" type="mediumType" use="required"/>
1005 </xs:complexType>
1006
1007 <xs:complexType name="SecretKeyProtectionType">
1008   <xs:sequence>
1009     <xs:element ref="KeyActivation" minOccurs="0"/>
1010     <xs:element ref="KeyStorage" minOccurs="0"/>
1011     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1012   </xs:sequence>
1013 </xs:complexType>
1014
1015 <xs:complexType name="SecurityAuditType">
1016   <xs:sequence>
1017     <xs:element ref="SwitchAudit" minOccurs="0"/>
1018     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1019   </xs:sequence>
1020 </xs:complexType>
1021
1022 <xs:complexType name="ExtensionOnlyType">
1023   <xs:sequence>
1024     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1025   </xs:sequence>
1026 </xs:complexType>
1027
1028 <xs:element name="Extension" type="ExtensionType"/>
1029
1030 <xs:complexType name="ExtensionType">
1031   <xs:sequence>
1032     <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
1033   </xs:sequence>
1034 </xs:complexType>
1035
1036 </xs:schema>
1037
1038
1039 <?xml version="1.0" encoding="UTF-8"?>
1040 <xs:schema
1041   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
1042   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1043   xmlns="urn:oasis:names:tc:SAML:2.0:ac"
1044   blockDefault="substitution"
1045   version="2.0">
1046
1047   <xs:annotation>
1048     <xs:documentation>
1049       Document identifier: saml-schema-authn-context-2.0
1050       Location: http://docs.oasis-open.org/security/saml/v2.0/
1051       Revision history:

```

1052
1053
1054
1055
1056
1057
1058
1059
1060
1061

```
V2.0 (March, 2005):  
    New core authentication context schema for SAML V2.0.  
    This is just an include of all types from the schema  
    referred to in the include statement below.  
</xs:documentation>  
</xs:annotation>  
  
<xs:include schemaLocation="saml-schema-authn-context-types-2.0.xsd"/>  
</xs:schema>
```

1062 **3 Authentication Context Classes**

1063 The number of permutations of different characteristics ensures that there is a theoretically infinite number
1064 of unique authentication contexts. The implication is that, in theory, any particular relying party would be
1065 expected to be able to parse arbitrary authentication context declarations and, more importantly, to
1066 analyze the declaration in order to assess the “quality” of the associated authentication assertion. Making
1067 such an assessment is non-trivial.

1068 Fortunately, an optimization is possible. In practice many authentication contexts will fall into categories
1069 determined by industry practices and technology. For instance, many B2C web browser authentication
1070 contexts will be (partially) defined by the principal authenticating to the authentication authority through the
1071 presentation of a password over an SSL protected session. In the enterprise world, certificate-based
1072 authentication will be common. Of course, the full authentication context is not limited to the specifics of
1073 how the principal authenticated. Nevertheless, the authentication method is often the most visible
1074 characteristic and as such, can serve as a useful classifier for a class of related authentication contexts.

1075 The concept is expressed in this specification as a definition of a series of authentication context classes.
1076 Each class defines a proper subset of the full set of authentication contexts. Classes have been chosen
1077 as representative of the current practices and technologies for authentication technologies, and provide
1078 asserting and relying parties a convenient shorthand when referring to authentication context issues.

1079 For instance, an authentication authority may include with the complete authentication context declaration
1080 it provides to a relying party an assertion that the authentication context also belongs to an authentication
1081 context class. For some relying parties, this assertion is sufficient detail for it to be able to assign an
1082 appropriate level of confidence to the associated authentication assertion. Other relying parties might
1083 prefer to examine the complete authentication context declaration itself. Likewise, the ability to refer to an
1084 authentication context class rather than being required to list the complete details of a specific
1085 authentication context declaration will simplify how the relying party can express its desires and/or
1086 requirements to an authentication authority.

1087 **3.1 Advantages of Authentication Context Classes**

1088 The introduction of the additional layer of classes and the definition of an initial list of representative and
1089 flexible classes are expected to:

- 1090 • Make it easier for the authentication authority and relying party to come to an agreement on what are
1091 acceptable authentication contexts by giving them a framework for discussion.
- 1092 • Make it easier for relying parties to indicate their preferences when requesting a step-up
1093 authentication assertion from an authentication authority.
- 1094 • Simplify for relying parties the burden of processing authentication context declarations by giving
1095 them the option of being satisfied by the associated class.
- 1096 • Insulate relying parties from the impact of new authentication technologies.
- 1097 • Make it easier for authentication authorities to publish their authentication capabilities, for example,
1098 through WSDL.

1099 **3.2 Processing Rules**

1100 Further processing rules for authentication context classes are described in the SAML assertions and
1101 protocols specification [SAMLCore]. Note that in most respects, these processing rules amount to
1102 deployments sharing common interpretations of the relative strength or quality of particular authentication
1103 context classes and cannot be expressed in absolute terms or provided as rules that implementations
1104 must follow.

1105 3.3 Extensibility

1106 As does the core authentication context declaration schema, the separate authentication context class
1107 schemas allow the <Extension> element in certain locations of the tree structure. In general, where the
1108 <Extension> element occurred as a child of an <xs:choice> element, this option was removed in
1109 creating the appropriate class schema definition as a restriction of the base type. When the
1110 <Extension> element occurred as an optional child of an <xs:sequence> element, the <Extension>
1111 element was allowed to remain in addition to any required elements.

1112 Consequently, authentication context declarations can include the <Extension> element (with additional
1113 elements in different namespaces) and still conform to authentication context class schemas (if they meet
1114 the other requirements of the schema of course).

1115 The authentication context class schemas restrict type definitions in the base authentication context
1116 schema. As an extension point, the authentication context class schemas themselves can be further
1117 restricted – their type definitions serving as base types in some other schema (potentially defined by
1118 some community wishing a more tightly defined authentication context class). To prevent logical
1119 inconsistencies, any such schema extensions can only further constrain the type definitions of the class
1120 schema. To enforce this constraint, the authentication context class schemas are defined with the
1121 `finalDefault="extension"` attribute on the <schema> element to prevent this type of derivation.

1122 Additional authentication context classes MAY be developed by groups other than the Security Services
1123 Technical Committee. OASIS members may wish to document and submit them for consideration by the
1124 SSTC in a future version of the specification, and other groups may simply wish to inform the committee
1125 of their work. Please refer to the SSTC web site for further details.

1126 Guidelines for the specification of new context classes are as follows:

- 1127 • Specify a URI that uniquely identifies the context class.
- 1128 • Provide contact information for the author of the class.
- 1129 • Provide a textual description of the circumstances under which this class should be used.
- 1130 • Provide a valid XML schema [Schema1] document implementing the class.

1131 Authors of new classes are encouraged to review the classes defined within this specification in order to
1132 guide their work.

1133 3.4 Schemas

1134 Authentication context classes are listed in the following sub-sections. The classes are listed in
1135 alphabetical order; no other ranking is implied by the order of classes. Classes are uniquely identified by
1136 URIs with the following initial stem:

```
1137 urn:oasis:names:tc:SAML:2.0:ac:classes
```

1138 The class schemas are defined as restrictions of parts of the base authentication context "types" schema.
1139 XML instances that validate against a given authentication context class schema are said to *conform* to
1140 that authentication context class.

1141 Note that because the class schema imports and redefines the elements and types into the class schema
1142 namespace, a class-conforming authentication context declaration does not simultaneously validate
1143 against the base authentication context schema.

1144 3.4.1 Internet Protocol

1145 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol

1146 Note that this URI is also used as the target namespace in the corresponding authentication context class
1147 schema document [SAMLAC-IP].

1148 The Internet Protocol class is applicable when a principal is authenticated through the use of a provided IP
1149 address.

```
1150 <?xml version="1.0" encoding="UTF-8"?>
1151
1152 <xs:schema
1153   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1154   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1155   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1156   finalDefault="extension"
1157   blockDefault="substitution"
1158   version="2.0">
1159
1160   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
1161
1162     <xs:annotation>
1163       <xs:documentation>
1164         Class identifier:
1165 urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
1166         Document identifier: saml-schema-authn-context-ip-2.0
1167         Location: http://docs.oasis-open.org/security/saml/v2.0/
1168         Revision history:
1169           V2.0 (March, 2005):
1170             New authentication context class schema for SAML V2.0.
1171       </xs:documentation>
1172     </xs:annotation>
1173
1174     <xs:complexType name="AuthnContextDeclarationBaseType">
1175       <xs:complexContent>
1176         <xs:restriction base="AuthnContextDeclarationBaseType">
1177           <xs:sequence>
1178             <xs:element ref="Identification" minOccurs="0"/>
1179             <xs:element ref="TechnicalProtection" minOccurs="0"/>
1180             <xs:element ref="OperationalProtection" minOccurs="0"/>
1181             <xs:element ref="AuthnMethod"/>
1182             <xs:element ref="GoverningAgreements" minOccurs="0"/>
1183             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1184           </xs:sequence>
1185           <xs:attribute name="ID" type="xs:ID" use="optional"/>
1186         </xs:restriction>
1187       </xs:complexContent>
1188     </xs:complexType>
1189
1190     <xs:complexType name="AuthnMethodBaseType">
1191       <xs:complexContent>
1192         <xs:restriction base="AuthnMethodBaseType">
1193           <xs:sequence>
1194             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1195             <xs:element ref="Authenticator"/>
1196             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1197             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1198           </xs:sequence>
1199         </xs:restriction>
1200       </xs:complexContent>
1201     </xs:complexType>
1202
1203     <xs:complexType name="AuthenticatorBaseType">
1204       <xs:complexContent>
1205         <xs:restriction base="AuthenticatorBaseType">
1206           <xs:sequence>
1207             <xs:element ref="IPAddress"/>
1208           </xs:sequence>
1209         </xs:restriction>
1210       </xs:complexContent>
1211     </xs:complexType>
1212
1213   </xs:redefine>
```

1214
1215 </xs:schema>

1216 3.4.2 InternetProtocolPassword

1217 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword

1218 Note that this URI is also used as the target namespace in the corresponding authentication context class
1219 schema document [SAMLAC-IPP].

1220 The Internet Protocol Password class is applicable when a principal is authenticated through the use of a
1221 provided IP address, in addition to a username/password.

```
1222 <?xml version="1.0" encoding="UTF-8"?>
1223
1224 <xs:schema
1225   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassw
1226   ord"
1227   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1228   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1229   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
1230   finalDefault="extension"
1231   blockDefault="substitution"
1232   version="2.0">
1233
1234   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
1235
1236     <xs:annotation>
1237       <xs:documentation>
1238         Class identifier:
1239 urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
1240         Document identifier: saml-schema-authn-context-ippword-2.0
1241         Location: http://docs.oasis-open.org/security/saml/v2.0/
1242         Revision history:
1243           V2.0 (March, 2005):
1244             New authentication context class schema for SAML V2.0.
1245       </xs:documentation>
1246     </xs:annotation>
1247
1248     <xs:complexType name="AuthnContextDeclarationBaseType">
1249       <xs:complexContent>
1250         <xs:restriction base="AuthnContextDeclarationBaseType">
1251           <xs:sequence>
1252             <xs:element ref="Identification" minOccurs="0"/>
1253             <xs:element ref="TechnicalProtection" minOccurs="0"/>
1254             <xs:element ref="OperationalProtection" minOccurs="0"/>
1255             <xs:element ref="AuthnMethod"/>
1256             <xs:element ref="GoverningAgreements" minOccurs="0"/>
1257             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1258           </xs:sequence>
1259           <xs:attribute name="ID" type="xs:ID" use="optional"/>
1260         </xs:restriction>
1261       </xs:complexContent>
1262     </xs:complexType>
1263
1264     <xs:complexType name="AuthnMethodBaseType">
1265       <xs:complexContent>
1266         <xs:restriction base="AuthnMethodBaseType">
1267           <xs:sequence>
1268             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1269             <xs:element ref="Authenticator"/>
1270             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1271             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1272           </xs:sequence>
1273         </xs:restriction>
1274       </xs:complexContent>
```



```

1275     </xs:complexType>
1276
1277     <xs:complexType name="AuthenticatorBaseType">
1278       <xs:complexContent>
1279         <xs:restriction base="AuthenticatorBaseType">
1280           <xs:sequence>
1281             <xs:element ref="Password"/>
1282             <xs:element ref="IPAddress"/>
1283             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1284           </xs:sequence>
1285         </xs:restriction>
1286       </xs:complexContent>
1287     </xs:complexType>
1288
1289   </xs:redefine>
1290
1291 </xs:schema>

```

1292 3.4.3 Kerberos

1293 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

1294 Note that this URI is also used as the target namespace in the corresponding authentication context class
 1295 schema document [SAMLAC-Kerb].

1296 This class is applicable when the principal has authenticated using a password to a local authentication
 1297 authority, in order to acquire a Kerberos ticket. That Kerberos ticket is then used for subsequent network
 1298 authentication.

1299 **Note:** It is possible for the authentication authority to indicate (via this context class) a pre-
 1300 authentication data type which was used by the Kerberos Key Distribution Center [RFC 1510]
 1301 when authenticating the principal. The method used by the authentication authority to obtain this
 1302 information is outside of the scope of this specification, but it is strongly recommended that a
 1303 trusted method be deployed to pass the pre-authentication data type and any other Kerberos
 1304 related context details (e.g. ticket lifetime) to the authentication authority.

```

1305 <?xml version="1.0" encoding="UTF-8"?>
1306
1307 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1308   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1309   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1310   finalDefault="extension"
1311   blockDefault="substitution"
1312   version="2.0">
1313
1314   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
1315
1316     <xs:annotation>
1317       <xs:documentation>
1318         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
1319         Document identifier: saml-schema-authn-context-kerberos-2.0
1320         Location: http://docs.oasis-open.org/security/saml/v2.0/
1321         Revision history:
1322           V2.0 (March, 2005):
1323             New authentication context class schema for SAML V2.0.
1324       </xs:documentation>
1325     </xs:annotation>
1326
1327     <xs:complexType name="AuthnContextDeclarationBaseType">
1328       <xs:complexContent>
1329         <xs:restriction base="AuthnContextDeclarationBaseType">
1330           <xs:sequence>
1331             <xs:element ref="Identification" minOccurs="0"/>
1332             <xs:element ref="TechnicalProtection" minOccurs="0"/>
1333             <xs:element ref="OperationalProtection" minOccurs="0"/>

```

```

1334         <xs:element ref="AuthnMethod"/>
1335         <xs:element ref="GoverningAgreements" minOccurs="0"/>
1336         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1337     </xs:sequence>
1338     <xs:attribute name="ID" type="xs:ID" use="optional"/>
1339 </xs:restriction>
1340 </xs:complexContent>
1341 </xs:complexType>
1342
1343 <xs:complexType name="AuthnMethodBaseType">
1344     <xs:complexContent>
1345         <xs:restriction base="AuthnMethodBaseType">
1346             <xs:sequence>
1347                 <xs:element ref="PrincipalAuthenticationMechanism"/>
1348                 <xs:element ref="Authenticator"/>
1349                 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1350                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1351             </xs:sequence>
1352         </xs:restriction>
1353     </xs:complexContent>
1354 </xs:complexType>
1355
1356 <xs:complexType name="PrincipalAuthenticationMechanismType">
1357     <xs:complexContent>
1358         <xs:restriction base="PrincipalAuthenticationMechanismType">
1359             <xs:sequence>
1360                 <xs:element ref="RestrictedPassword"/>
1361             </xs:sequence>
1362             <xs:attribute name="preauth" type="xs:integer" use="optional"/>
1363         </xs:restriction>
1364     </xs:complexContent>
1365 </xs:complexType>
1366
1367 <xs:complexType name="AuthenticatorBaseType">
1368     <xs:complexContent>
1369         <xs:restriction base="AuthenticatorBaseType">
1370             <xs:sequence>
1371                 <xs:element ref="SharedSecretChallengeResponse"/>
1372             </xs:sequence>
1373         </xs:restriction>
1374     </xs:complexContent>
1375 </xs:complexType>
1376
1377 <xs:complexType name="SharedSecretChallengeResponseType">
1378     <xs:complexContent>
1379         <xs:restriction base="SharedSecretChallengeResponseType">
1380             <xs:attribute name="method" type="xs:anyURI"
1381 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
1382         </xs:restriction>
1383     </xs:complexContent>
1384 </xs:complexType>
1385
1386 </xs:redefine>
1387
1388 </xs:schema>

```

1389

1390 An example of an XML instance conforming to this class schema is as follows:

```
1391 <AuthenticationContextDeclaration
1392   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos">
1393
1394   <AuthnMethod>
1395
1396     <PrincipalAuthenticationMechanism preauth="0">
1397       <RestrictedPassword>
1398         <Length min="4"/>
1399       </RestrictedPassword>
1400     </PrincipalAuthenticationMechanism>
1401
1402     <Authenticator>
1403       <AuthenticatorSequence>
1404         <SharedSecretChallengeResponse
1405 method="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
1406       </AuthenticatorSequence>
1407     </Authenticator>
1408
1409   </AuthnMethod>
1410
1411 </AuthenticationContextDeclaration>
```

1412 **3.4.4 MobileOneFactorUnregistered**

1413 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered

1414 Note that this URI is also used as the target namespace in the corresponding authentication context class
1415 schema document [SAMLAC-MOFU].

1416 Reflects no mobile customer registration procedures and an authentication of the mobile device without
1417 requiring explicit end-user interaction. This context class authenticates only the device and never the user;
1418 it is useful when services other than the mobile operator want to add a secure device authentication to
1419 their authentication process.

```
1420 <?xml version="1.0" encoding="UTF-8"?>
1421
1422 <xs:schema
1423   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregi
1424 stered"
1425   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1426   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered"
1427   finalDefault="extension"
1428   blockDefault="substitution"
1429   version="2.0">
1430
1431   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
1432
1433     <xs:annotation>
1434       <xs:documentation>
1435         Class identifier:
1436 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
1437         Document identifier: saml-schema-authn-context-mobileonefactor-unreg-2.0
1438         Location: http://docs.oasis-open.org/security/saml/v2.0/
1439         Revision history:
1440           V2.0 (March, 2005):
1441             New authentication context class schema for SAML V2.0.
1442       </xs:documentation>
1443     </xs:annotation>
1444
1445     <xs:complexType name="AuthnContextDeclarationBaseType">
1446       <xs:complexContent>
1447         <xs:restriction base="AuthnContextDeclarationBaseType">
1448           <xs:sequence>
1449             <xs:element ref="Identification" minOccurs="0"/>
```

```

1450     <xs:element ref="TechnicalProtection" minOccurs="0"/>
1451     <xs:element ref="OperationalProtection" minOccurs="0"/>
1452     <xs:element ref="AuthnMethod"/>
1453     <xs:element ref="GoverningAgreements" minOccurs="0"/>
1454     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1455   </xs:sequence>
1456   <xs:attribute name="ID" type="xs:ID" use="optional"/>
1457 </xs:restriction>
1458 </xs:complexContent>
1459 </xs:complexType>
1460
1461 <xs:complexType name="AuthnMethodBaseType">
1462   <xs:complexContent>
1463     <xs:restriction base="AuthnMethodBaseType">
1464       <xs:sequence>
1465         <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1466         <xs:element ref="Authenticator"/>
1467         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1468         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1469       </xs:sequence>
1470     </xs:restriction>
1471   </xs:complexContent>
1472 </xs:complexType>
1473
1474 <xs:complexType name="AuthenticatorBaseType">
1475   <xs:complexContent>
1476     <xs:restriction base="AuthenticatorBaseType">
1477       <xs:sequence>
1478         <xs:choice>
1479           <xs:element ref="DigSig"/>
1480           <xs:element ref="ZeroKnowledge"/>
1481           <xs:element ref="SharedSecretChallengeResponse"/>
1482           <xs:element ref="SharedSecretDynamicPlaintext"/>
1483           <xs:element ref="AsymmetricDecryption"/>
1484           <xs:element ref="AsymmetricKeyAgreement"/>
1485         </xs:choice>
1486         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1487       </xs:sequence>
1488     </xs:restriction>
1489   </xs:complexContent>
1490 </xs:complexType>
1491
1492 <xs:complexType name="AuthenticatorTransportProtocolType">
1493   <xs:complexContent>
1494     <xs:restriction base="AuthenticatorTransportProtocolType">
1495       <xs:sequence>
1496         <xs:choice>
1497           <xs:element ref="SSL"/>
1498           <xs:element ref="MobileNetworkNoEncryption"/>
1499           <xs:element ref="MobileNetworkRadioEncryption"/>
1500           <xs:element ref="MobileNetworkEndToEndEncryption"/>
1501           <xs:element ref="WTLS"/>
1502         </xs:choice>
1503         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1504       </xs:sequence>
1505     </xs:restriction>
1506   </xs:complexContent>
1507 </xs:complexType>
1508
1509 <xs:complexType name="OperationalProtectionType">
1510   <xs:complexContent>
1511     <xs:restriction base="OperationalProtectionType">
1512       <xs:sequence>
1513         <xs:element ref="SecurityAudit"/>
1514         <xs:element ref="DeactivationCallCenter"/>
1515         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1516       </xs:sequence>

```

```

1517     </xs:restriction>
1518   </xs:complexContent>
1519 </xs:complexType>
1520
1521 <xs:complexType name="TechnicalProtectionBaseType">
1522   <xs:complexContent>
1523     <xs:restriction base="TechnicalProtectionBaseType">
1524       <xs:sequence>
1525         <xs:choice>
1526           <xs:element ref="PrivateKeyProtection"/>
1527           <xs:element ref="SecretKeyProtection"/>
1528         </xs:choice>
1529         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1530       </xs:sequence>
1531     </xs:restriction>
1532   </xs:complexContent>
1533 </xs:complexType>
1534
1535 <xs:complexType name="PrivateKeyProtectionType">
1536   <xs:complexContent>
1537     <xs:restriction base="PrivateKeyProtectionType">
1538       <xs:sequence>
1539         <xs:element ref="KeyStorage"/>
1540         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1541       </xs:sequence>
1542     </xs:restriction>
1543   </xs:complexContent>
1544 </xs:complexType>
1545
1546 <xs:complexType name="SecretKeyProtectionType">
1547   <xs:complexContent>
1548     <xs:restriction base="SecretKeyProtectionType">
1549       <xs:sequence>
1550         <xs:element ref="KeyStorage"/>
1551         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1552       </xs:sequence>
1553     </xs:restriction>
1554   </xs:complexContent>
1555 </xs:complexType>
1556
1557 <xs:complexType name="KeyStorageType">
1558   <xs:complexContent>
1559     <xs:restriction base="KeyStorageType">
1560       <xs:attribute name="medium" use="required">
1561         <xs:simpleType>
1562           <xs:restriction base="mediumType">
1563             <xs:enumeration value="MobileDevice"/>
1564             <xs:enumeration value="MobileAuthCard"/>
1565             <xs:enumeration value="smartcard"/>
1566           </xs:restriction>
1567         </xs:simpleType>
1568       </xs:attribute>
1569     </xs:restriction>
1570   </xs:complexContent>
1571 </xs:complexType>
1572
1573 <xs:complexType name="SecurityAuditType">
1574   <xs:complexContent>
1575     <xs:restriction base="SecurityAuditType">
1576       <xs:sequence>
1577         <xs:element ref="SwitchAudit"/>
1578         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1579       </xs:sequence>
1580     </xs:restriction>
1581   </xs:complexContent>
1582 </xs:complexType>
1583

```

```

1584     <xs:complexType name="IdentificationType">
1585       <xs:complexContent>
1586         <xs:restriction base="IdentificationType">
1587           <xs:sequence>
1588             <xs:element ref="GoverningAgreements"/>
1589             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1590           </xs:sequence>
1591           <xs:attribute name="nym">
1592             <xs:simpleType>
1593               <xs:restriction base="nymType">
1594                 <xs:enumeration value="anonymity"/>
1595                 <xs:enumeration value="pseudonymity"/>
1596               </xs:restriction>
1597             </xs:simpleType>
1598           </xs:attribute>
1599         </xs:restriction>
1600       </xs:complexContent>
1601     </xs:complexType>
1602
1603   </xs:redefine>
1604
1605 </xs:schema>

```

1606 3.4.5 MobileTwoFactorUnregistered

1607 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered

1608 Note that this URI is also used as the target namespace in the corresponding authentication context class
1609 schema document [SAMLAC-MTFU].

1610 Reflects no mobile customer registration procedures and a two-factor based authentication, such as
1611 secure device and user PIN. This context class is useful when a service other than the mobile operator
1612 wants to link their customer ID to a mobile supplied two-factor authentication service by capturing mobile
1613 phone data at enrollment.

```

1614 <?xml version="1.0" encoding="UTF-8"?>
1615
1616 <xs:schema
1617   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregist
1618   ered"
1619   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1620   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered"
1621   finalDefault="extension"
1622   blockDefault="substitution"
1623   version="2.0">
1624
1625   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
1626
1627     <xs:annotation>
1628       <xs:documentation>
1629         Class identifier:
1630 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
1631         Document identifier: saml-schema-authn-context-mobiletwofactor-unreg-2.0
1632         Location: http://docs.oasis-open.org/security/saml/v2.0/
1633         Revision history:
1634           V2.0 (March, 2005):
1635             New authentication context class schema for SAML V2.0.
1636       </xs:documentation>
1637     </xs:annotation>
1638
1639     <xs:complexType name="AuthnContextDeclarationBaseType">
1640       <xs:complexContent>
1641         <xs:restriction base="AuthnContextDeclarationBaseType">
1642           <xs:sequence>
1643             <xs:element ref="Identification" minOccurs="0"/>
1644             <xs:element ref="TechnicalProtection" minOccurs="0"/>

```

```

1645         <xs:element ref="OperationalProtection" minOccurs="0"/>
1646         <xs:element ref="AuthnMethod"/>
1647         <xs:element ref="GoverningAgreements" minOccurs="0"/>
1648         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1649     </xs:sequence>
1650     <xs:attribute name="ID" type="xs:ID" use="optional"/>
1651 </xs:restriction>
1652 </xs:complexContent>
1653 </xs:complexType>
1654
1655 <xs:complexType name="AuthnMethodBaseType">
1656     <xs:complexContent>
1657         <xs:restriction base="AuthnMethodBaseType">
1658             <xs:sequence>
1659                 <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1660                 <xs:element ref="Authenticator"/>
1661                 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1662                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1663             </xs:sequence>
1664         </xs:restriction>
1665     </xs:complexContent>
1666 </xs:complexType>
1667
1668 <xs:complexType name="AuthenticatorBaseType">
1669     <xs:complexContent>
1670         <xs:restriction base="AuthenticatorBaseType">
1671             <xs:sequence>
1672                 <xs:choice>
1673                     <xs:element ref="DigSig"/>
1674                     <xs:element ref="ZeroKnowledge"/>
1675                     <xs:element ref="SharedSecretChallengeResponse"/>
1676                     <xs:element ref="SharedSecretDynamicPlaintext"/>
1677                     <xs:element ref="AsymmetricDecryption"/>
1678                     <xs:element ref="AsymmetricKeyAgreement"/>
1679                     <xs:element ref="ComplexAuthenticator"/>
1680                 </xs:choice>
1681                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1682             </xs:sequence>
1683         </xs:restriction>
1684     </xs:complexContent>
1685 </xs:complexType>
1686
1687 <xs:complexType name="ComplexAuthenticatorType">
1688     <xs:complexContent>
1689         <xs:restriction base="ComplexAuthenticatorType">
1690             <xs:sequence>
1691                 <xs:choice>
1692                     <xs:element ref="SharedSecretChallengeResponse"/>
1693                     <xs:element ref="SharedSecretDynamicPlaintext"/>
1694                 </xs:choice>
1695                 <xs:element ref="Password"/>
1696             </xs:sequence>
1697         </xs:restriction>
1698     </xs:complexContent>
1699 </xs:complexType>
1700
1701 <xs:complexType name="AuthenticatorTransportProtocolType">
1702     <xs:complexContent>
1703         <xs:restriction base="AuthenticatorTransportProtocolType">
1704             <xs:sequence>
1705                 <xs:choice>
1706                     <xs:element ref="SSL"/>
1707                     <xs:element ref="MobileNetworkNoEncryption"/>
1708                     <xs:element ref="MobileNetworkRadioEncryption"/>
1709                     <xs:element ref="MobileNetworkEndToEndEncryption"/>
1710                     <xs:element ref="WTLS"/>
1711                 </xs:choice>

```

```

1712         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1713     </xs:sequence>
1714 </xs:restriction>
1715 </xs:complexContent>
1716 </xs:complexType>
1717
1718 <xs:complexType name="OperationalProtectionType">
1719     <xs:complexContent>
1720         <xs:restriction base="OperationalProtectionType">
1721             <xs:sequence>
1722                 <xs:element ref="SecurityAudit"/>
1723                 <xs:element ref="DeactivationCallCenter"/>
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="TechnicalProtectionBaseType">
1731     <xs:complexContent>
1732         <xs:restriction base="TechnicalProtectionBaseType">
1733             <xs:sequence>
1734                 <xs:choice>
1735                     <xs:element ref="PrivateKeyProtection"/>
1736                     <xs:element ref="SecretKeyProtection"/>
1737                 </xs:choice>
1738                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1739             </xs:sequence>
1740         </xs:restriction>
1741     </xs:complexContent>
1742 </xs:complexType>
1743
1744 <xs:complexType name="PrivateKeyProtectionType">
1745     <xs:complexContent>
1746         <xs:restriction base="PrivateKeyProtectionType">
1747             <xs:sequence>
1748                 <xs:element ref="KeyActivation"/>
1749                 <xs:element ref="KeyStorage"/>
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="SecretKeyProtectionType">
1757     <xs:complexContent>
1758         <xs:restriction base="SecretKeyProtectionType">
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="KeyStorageType">
1769     <xs:complexContent>
1770         <xs:restriction base="KeyStorageType">
1771             <xs:attribute name="medium" use="required">
1772                 <xs:simpleType>
1773                     <xs:restriction base="mediumType">
1774                         <xs:enumeration value="MobileDevice"/>
1775                         <xs:enumeration value="MobileAuthCard"/>
1776                         <xs:enumeration value="smartcard"/>
1777                     </xs:restriction>
1778                 </xs:simpleType>

```



```

1779     </xs:attribute>
1780     </xs:restriction>
1781     </xs:complexContent>
1782 </xs:complexType>
1783
1784 <xs:complexType name="SecurityAuditType">
1785   <xs:complexContent>
1786     <xs:restriction base="SecurityAuditType">
1787       <xs:sequence>
1788         <xs:element ref="SwitchAudit"/>
1789         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1790       </xs:sequence>
1791     </xs:restriction>
1792   </xs:complexContent>
1793 </xs:complexType>
1794
1795 <xs:complexType name="IdentificationType">
1796   <xs:complexContent>
1797     <xs:restriction base="IdentificationType">
1798       <xs:sequence>
1799         <xs:element ref="GoverningAgreements"/>
1800         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1801       </xs:sequence>
1802       <xs:attribute name="nym">
1803         <xs:simpleType>
1804           <xs:restriction base="nymType">
1805             <xs:enumeration value="anonymity"/>
1806             <xs:enumeration value="pseudonymity"/>
1807           </xs:restriction>
1808         </xs:simpleType>
1809       </xs:attribute>
1810     </xs:restriction>
1811   </xs:complexContent>
1812 </xs:complexType>
1813
1814 </xs:redefine>
1815
1816 </xs:schema>

```

1817 3.4.6 MobileOneFactorContract

1818 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract

1819 Note that this URI is also used as the target namespace in the corresponding authentication context class
1820 schema document [SAMLAC-MOFC].

1821 Reflects mobile contract customer registration procedures and a single factor authentication. For example,
1822 a digital signing device with tamper resistant memory for key storage, such as the mobile MSISDN, but no
1823 required PIN or biometric for real-time user authentication.

```

1824 <?xml version="1.0" encoding="UTF-8"?>
1825
1826 <xs:schema
1827   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
1828 <
1829   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1830   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
1831   finalDefault="extension"
1832   blockDefault="substitution"
1833   version="2.0">
1834
1835   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
1836
1837     <xs:annotation>
1838       <xs:documentation>

```

```

1839     Class identifier:
1840 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
1841     Document identifier: saml-schema-authn-context-mobileonefactor-reg-2.0
1842     Location: http://docs.oasis-open.org/security/saml/v2.0/
1843     Revision history:
1844         V2.0 (March, 2005):
1845         New authentication context class schema for SAML V2.0.
1846     </xs:documentation>
1847 </xs:annotation>
1848
1849     <xs:complexType name="AuthnContextDeclarationBaseType">
1850     <xs:complexContent>
1851     <xs:restriction base="AuthnContextDeclarationBaseType">
1852     <xs:sequence>
1853     <xs:element ref="Identification" minOccurs="0"/>
1854     <xs:element ref="TechnicalProtection" minOccurs="0"/>
1855     <xs:element ref="OperationalProtection" minOccurs="0"/>
1856     <xs:element ref="AuthnMethod"/>
1857     <xs:element ref="GoverningAgreements" minOccurs="0"/>
1858     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1859     </xs:sequence>
1860     <xs:attribute name="ID" type="xs:ID" use="optional"/>
1861     </xs:restriction>
1862     </xs:complexContent>
1863 </xs:complexType>
1864
1865     <xs:complexType name="AuthnMethodBaseType">
1866     <xs:complexContent>
1867     <xs:restriction base="AuthnMethodBaseType">
1868     <xs:sequence>
1869     <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
1870     <xs:element ref="Authenticator"/>
1871     <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
1872     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1873     </xs:sequence>
1874     </xs:restriction>
1875     </xs:complexContent>
1876 </xs:complexType>
1877
1878     <xs:complexType name="AuthenticatorBaseType">
1879     <xs:complexContent>
1880     <xs:restriction base="AuthenticatorBaseType">
1881     <xs:sequence>
1882     <xs:choice>
1883     <xs:element ref="DigSig"/>
1884     <xs:element ref="ZeroKnowledge"/>
1885     <xs:element ref="SharedSecretChallengeResponse"/>
1886     <xs:element ref="SharedSecretDynamicPlaintext"/>
1887     <xs:element ref="AsymmetricDecryption"/>
1888     <xs:element ref="AsymmetricKeyAgreement"/>
1889     </xs:choice>
1890     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1891     </xs:sequence>
1892     </xs:restriction>
1893     </xs:complexContent>
1894 </xs:complexType>
1895
1896     <xs:complexType name="AuthenticatorTransportProtocolType">
1897     <xs:complexContent>
1898     <xs:restriction base="AuthenticatorTransportProtocolType">
1899     <xs:sequence>
1900     <xs:choice>
1901     <xs:element ref="SSL"/>
1902     <xs:element ref="MobileNetworkNoEncryption"/>
1903     <xs:element ref="MobileNetworkRadioEncryption"/>
1904     <xs:element ref="MobileNetworkEndToEndEncryption"/>
1905     <xs:element ref="WTLS"/>

```

```

1906         </xs:choice>
1907         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1908     </xs:sequence>
1909 </xs:restriction>
1910 </xs:complexContent>
1911 </xs:complexType>
1912
1913 <xs:complexType name="OperationalProtectionType">
1914     <xs:complexContent>
1915         <xs:restriction base="OperationalProtectionType">
1916             <xs:sequence>
1917                 <xs:element ref="SecurityAudit"/>
1918                 <xs:element ref="DeactivationCallCenter"/>
1919                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1920             </xs:sequence>
1921         </xs:restriction>
1922     </xs:complexContent>
1923 </xs:complexType>
1924
1925 <xs:complexType name="TechnicalProtectionBaseType">
1926     <xs:complexContent>
1927         <xs:restriction base="TechnicalProtectionBaseType">
1928             <xs:sequence>
1929                 <xs:choice>
1930                     <xs:element ref="PrivateKeyProtection"/>
1931                     <xs:element ref="SecretKeyProtection"/>
1932                 </xs:choice>
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="PrivateKeyProtectionType">
1940     <xs:complexContent>
1941         <xs:restriction base="PrivateKeyProtectionType">
1942             <xs:sequence>
1943                 <xs:element ref="KeyStorage"/>
1944                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1945             </xs:sequence>
1946         </xs:restriction>
1947     </xs:complexContent>
1948 </xs:complexType>
1949
1950 <xs:complexType name="SecretKeyProtectionType">
1951     <xs:complexContent>
1952         <xs:restriction base="SecretKeyProtectionType">
1953             <xs:sequence>
1954                 <xs:element ref="KeyStorage"/>
1955                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1956             </xs:sequence>
1957         </xs:restriction>
1958     </xs:complexContent>
1959 </xs:complexType>
1960
1961 <xs:complexType name="KeyStorageType">
1962     <xs:complexContent>
1963         <xs:restriction base="KeyStorageType">
1964             <xs:attribute name="medium" use="required">
1965                 <xs:simpleType>
1966                     <xs:restriction base="mediumType">
1967                         <xs:enumeration value="smartcard"/>
1968                         <xs:enumeration value="MobileDevice"/>
1969                         <xs:enumeration value="MobileAuthCard"/>
1970                     </xs:restriction>
1971                 </xs:simpleType>
1972             </xs:attribute>

```

```

1973     </xs:restriction>
1974   </xs:complexContent>
1975 </xs:complexType>
1976
1977   <xs:complexType name="SecurityAuditType">
1978     <xs:complexContent>
1979       <xs:restriction base="SecurityAuditType">
1980         <xs:sequence>
1981           <xs:element ref="SwitchAudit"/>
1982           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1983         </xs:sequence>
1984       </xs:restriction>
1985     </xs:complexContent>
1986   </xs:complexType>
1987
1988   <xs:complexType name="IdentificationType">
1989     <xs:complexContent>
1990       <xs:restriction base="IdentificationType">
1991         <xs:sequence>
1992           <xs:element ref="PhysicalVerification"/>
1993           <xs:element ref="WrittenConsent"/>
1994           <xs:element ref="GoverningAgreements"/>
1995           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1996         </xs:sequence>
1997         <xs:attribute name="nym">
1998           <xs:simpleType>
1999             <xs:restriction base="nymType">
2000               <xs:enumeration value="anonymity"/>
2001               <xs:enumeration value="veronymity"/>
2002               <xs:enumeration value="pseudonymity"/>
2003             </xs:restriction>
2004           </xs:simpleType>
2005         </xs:attribute>
2006       </xs:restriction>
2007     </xs:complexContent>
2008   </xs:complexType>
2009
2010 </xs:redefine>
2011
2012 </xs:schema>

```

2013 3.4.7 MobileTwoFactorContract

2014 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract

2015 Note that this URI is also used as the target namespace in the corresponding authentication context class
2016 schema document [SAMLAC-MTFC].

2017 Reflects mobile contract customer registration procedures and a two-factor based authentication. For
2018 example, a digital signing device with tamper resistant memory for key storage, such as a GSM SIM, that
2019 requires explicit proof of user identity and intent, such as a PIN or biometric.

```

2020 <?xml version="1.0" encoding="UTF-8"?>
2021
2022 <xs:schema
2023   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
2024   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2025   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
2026   finalDefault="extension"
2027   blockDefault="substitution"
2028   version="2.0">
2029
2030   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2031
2032     <xs:annotation>
2033       <xs:documentation>

```

```

2034         Class identifier:
2035 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
2036         Document identifier: saml-schema-authn-context-mobiletwofactor-reg-2.0
2037         Location: http://docs.oasis-open.org/security/saml/v2.0/
2038         Revision history:
2039             V2.0 (March, 2005):
2040             New authentication context class schema for SAML V2.0.
2041         </xs:documentation>
2042     </xs:annotation>
2043
2044     <xs:complexType name="AuthnContextDeclarationBaseType">
2045         <xs:complexContent>
2046             <xs:restriction base="AuthnContextDeclarationBaseType">
2047                 <xs:sequence>
2048                     <xs:element ref="Identification" minOccurs="0"/>
2049                     <xs:element ref="TechnicalProtection" minOccurs="0"/>
2050                     <xs:element ref="OperationalProtection" minOccurs="0"/>
2051                     <xs:element ref="AuthnMethod"/>
2052                     <xs:element ref="GoverningAgreements" minOccurs="0"/>
2053                     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2054                 </xs:sequence>
2055                 <xs:attribute name="ID" type="xs:ID" use="optional"/>
2056             </xs:restriction>
2057         </xs:complexContent>
2058     </xs:complexType>
2059
2060     <xs:complexType name="AuthnMethodBaseType">
2061         <xs:complexContent>
2062             <xs:restriction base="AuthnMethodBaseType">
2063                 <xs:sequence>
2064                     <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
2065                     <xs:element ref="Authenticator"/>
2066                     <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2067                     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2068                 </xs:sequence>
2069             </xs:restriction>
2070         </xs:complexContent>
2071     </xs:complexType>
2072
2073     <xs:complexType name="AuthenticatorBaseType">
2074         <xs:complexContent>
2075             <xs:restriction base="AuthenticatorBaseType">
2076                 <xs:sequence>
2077                     <xs:choice>
2078                         <xs:element ref="DigSig"/>
2079                         <xs:element ref="ZeroKnowledge"/>
2080                         <xs:element ref="SharedSecretChallengeResponse"/>
2081                         <xs:element ref="SharedSecretDynamicPlaintext"/>
2082                         <xs:element ref="AsymmetricDecryption"/>
2083                         <xs:element ref="AsymmetricKeyAgreement"/>
2084                         <xs:element ref="ComplexAuthenticator"/>
2085                     </xs:choice>
2086                     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2087                 </xs:sequence>
2088             </xs:restriction>
2089         </xs:complexContent>
2090     </xs:complexType>
2091
2092     <xs:complexType name="ComplexAuthenticatorType">
2093         <xs:complexContent>
2094             <xs:restriction base="ComplexAuthenticatorType">
2095                 <xs:sequence>
2096                     <xs:choice>
2097                         <xs:element ref="SharedSecretChallengeResponse"/>
2098                         <xs:element ref="SharedSecretDynamicPlaintext"/>
2099                     </xs:choice>
2100                     <xs:element ref="Password"/>

```

```

2101     </xs:sequence>
2102   </xs:restriction>
2103 </xs:complexContent>
2104 </xs:complexType>
2105
2106 <xs:complexType name="AuthenticatorTransportProtocolType">
2107   <xs:complexContent>
2108     <xs:restriction base="AuthenticatorTransportProtocolType">
2109       <xs:sequence>
2110         <xs:choice>
2111           <xs:element ref="SSL"/>
2112           <xs:element ref="MobileNetworkNoEncryption"/>
2113           <xs:element ref="MobileNetworkRadioEncryption"/>
2114           <xs:element ref="MobileNetworkEndToEndEncryption"/>
2115           <xs:element ref="WTLS"/>
2116         </xs:choice>
2117         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2118       </xs:sequence>
2119     </xs:restriction>
2120   </xs:complexContent>
2121 </xs:complexType>
2122
2123 <xs:complexType name="OperationalProtectionType">
2124   <xs:complexContent>
2125     <xs:restriction base="OperationalProtectionType">
2126       <xs:sequence>
2127         <xs:element ref="SecurityAudit"/>
2128         <xs:element ref="DeactivationCallCenter"/>
2129         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2130       </xs:sequence>
2131     </xs:restriction>
2132   </xs:complexContent>
2133 </xs:complexType>
2134
2135 <xs:complexType name="TechnicalProtectionBaseType">
2136   <xs:complexContent>
2137     <xs:restriction base="TechnicalProtectionBaseType">
2138       <xs:sequence>
2139         <xs:choice>
2140           <xs:element ref="PrivateKeyProtection"/>
2141           <xs:element ref="SecretKeyProtection"/>
2142         </xs:choice>
2143         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2144       </xs:sequence>
2145     </xs:restriction>
2146   </xs:complexContent>
2147 </xs:complexType>
2148
2149 <xs:complexType name="PrivateKeyProtectionType">
2150   <xs:complexContent>
2151     <xs:restriction base="PrivateKeyProtectionType">
2152       <xs:sequence>
2153         <xs:element ref="KeyActivation"/>
2154         <xs:element ref="KeyStorage"/>
2155         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2156       </xs:sequence>
2157     </xs:restriction>
2158   </xs:complexContent>
2159 </xs:complexType>
2160
2161 <xs:complexType name="SecretKeyProtectionType">
2162   <xs:complexContent>
2163     <xs:restriction base="SecretKeyProtectionType">
2164       <xs:sequence>
2165         <xs:element ref="KeyActivation"/>
2166         <xs:element ref="KeyStorage"/>
2167         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>

```

```

2168     </xs:sequence>
2169   </xs:restriction>
2170 </xs:complexContent>
2171 </xs:complexType>
2172
2173 <xs:complexType name="KeyStorageType">
2174   <xs:complexContent>
2175     <xs:restriction base="KeyStorageType">
2176       <xs:attribute name="medium" use="required">
2177         <xs:simpleType>
2178           <xs:restriction base="mediumType">
2179             <xs:enumeration value="MobileDevice"/>
2180             <xs:enumeration value="MobileAuthCard"/>
2181             <xs:enumeration value="smartcard"/>
2182           </xs:restriction>
2183         </xs:simpleType>
2184       </xs:attribute>
2185     </xs:restriction>
2186   </xs:complexContent>
2187 </xs:complexType>
2188
2189 <xs:complexType name="SecurityAuditType">
2190   <xs:complexContent>
2191     <xs:restriction base="SecurityAuditType">
2192       <xs:sequence>
2193         <xs:element ref="SwitchAudit"/>
2194         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2195       </xs:sequence>
2196     </xs:restriction>
2197   </xs:complexContent>
2198 </xs:complexType>
2199
2200 <xs:complexType name="IdentificationType">
2201   <xs:complexContent>
2202     <xs:restriction base="IdentificationType">
2203       <xs:sequence>
2204         <xs:element ref="PhysicalVerification"/>
2205         <xs:element ref="WrittenConsent"/>
2206         <xs:element ref="GoverningAgreements"/>
2207         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2208       </xs:sequence>
2209       <xs:attribute name="nym">
2210         <xs:simpleType>
2211           <xs:restriction base="nymType">
2212             <xs:enumeration value="anonymity"/>
2213             <xs:enumeration value="verinymity"/>
2214             <xs:enumeration value="pseudonymity"/>
2215           </xs:restriction>
2216         </xs:simpleType>
2217       </xs:attribute>
2218     </xs:restriction>
2219   </xs:complexContent>
2220 </xs:complexType>
2221
2222 </xs:redefine>
2223
2224 </xs:schema>

```

2225 3.4.8 Password

2226 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes>Password

2227 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2228 schema document [SAMLAC-Pass].

2229 The Password class is applicable when a principal authenticates to an authentication authority through the
2230 presentation of a password over an unprotected HTTP session.

```
2231 <?xml version="1.0" encoding="UTF-8"?>
2232
2233 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
2234   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2235   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
2236   finalDefault="extension"
2237   blockDefault="substitution"
2238   version="2.0">
2239
2240   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2241
2242     <xs:annotation>
2243       <xs:documentation>
2244         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Password
2245         Document identifier: saml-schema-authn-context-pword-2.0
2246         Location: http://docs.oasis-open.org/security/saml/v2.0/
2247         Revision history:
2248           V2.0 (March, 2005):
2249           New authentication context class schema for SAML V2.0.
2250       </xs:documentation>
2251     </xs:annotation>
2252
2253     <xs:complexType name="AuthnContextDeclarationBaseType">
2254       <xs:complexContent>
2255         <xs:restriction base="AuthnContextDeclarationBaseType">
2256           <xs:sequence>
2257             <xs:element ref="Identification" minOccurs="0"/>
2258             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2259             <xs:element ref="OperationalProtection" minOccurs="0"/>
2260             <xs:element ref="AuthnMethod"/>
2261             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2262             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2263           </xs:sequence>
2264           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2265         </xs:restriction>
2266       </xs:complexContent>
2267     </xs:complexType>
2268
2269     <xs:complexType name="AuthnMethodBaseType">
2270       <xs:complexContent>
2271         <xs:restriction base="AuthnMethodBaseType">
2272           <xs:sequence>
2273             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
2274             <xs:element ref="Authenticator"/>
2275             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2276             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2277           </xs:sequence>
2278         </xs:restriction>
2279       </xs:complexContent>
2280     </xs:complexType>
2281
2282     <xs:complexType name="AuthenticatorBaseType">
2283       <xs:complexContent>
2284         <xs:restriction base="AuthenticatorBaseType">
2285           <xs:sequence>
2286             <xs:element ref="RestrictedPassword"/>
2287           </xs:sequence>
2288         </xs:restriction>
2289       </xs:complexContent>
2290     </xs:complexType>
2291
2292   </xs:redefine>
2293 </xs:schema>
2294
```


2295 Following is an example of an XML instance that conforms to the context class schema:

```
2296 <AuthenticationContextDeclaration
2297   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password">
2298
2299   <AuthnMethod>
2300     <Authenticator>
2301       <AuthenticatorSequence>
2302         <RestrictedPassword>
2303           <Length min="4"/>
2304         </RestrictedPassword>
2305       </AuthenticatorSequence>
2306     </Authenticator>
2307   </AuthnMethod>
2308
2309 </AuthenticationContextDeclaration>
```

2310 **3.4.9 PasswordProtectedTransport**

2311 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

2312 Note that this URI is also used as the target namespace in the corresponding authentication context class
2313 schema document [SAMLAC-PPT].

2314 The PasswordProtectedTransport class is applicable when a principal authenticates to an authentication
2315 authority through the presentation of a password over a protected session.

```
2316 <?xml version="1.0" encoding="UTF-8"?>
2317
2318 <xs:schema
2319   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp
2320   ort"
2321   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2322   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
2323   finalDefault="extension"
2324   blockDefault="substitution"
2325   version="2.0">
2326
2327   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2328
2329     <xs:annotation>
2330       <xs:documentation>
2331         Class identifier:
2332         urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
2333         Document identifier: saml-schema-authn-context-ppt-2.0
2334         Location: http://docs.oasis-open.org/security/saml/v2.0/
2335         Revision history:
2336         V2.0 (March, 2005):
2337         New authentication context class schema for SAML V2.0.
2338       </xs:documentation>
2339     </xs:annotation>
2340
2341     <xs:complexType name="AuthnContextDeclarationBaseType">
2342       <xs:complexContent>
2343         <xs:restriction base="AuthnContextDeclarationBaseType">
2344           <xs:sequence>
2345             <xs:element ref="Identification" minOccurs="0"/>
2346             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2347             <xs:element ref="OperationalProtection" minOccurs="0"/>
2348             <xs:element ref="AuthnMethod"/>
2349             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2350             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2351           </xs:sequence>
2352           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2353         </xs:restriction>
2354       </xs:complexContent>
2355     </xs:complexType>
```

```

2356
2357     <xs:complexType name="AuthnMethodBaseType">
2358       <xs:complexContent>
2359         <xs:restriction base="AuthnMethodBaseType">
2360           <xs:sequence>
2361             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
2362             <xs:element ref="Authenticator"/>
2363             <xs:element ref="AuthenticatorTransportProtocol"/>
2364             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2365           </xs:sequence>
2366         </xs:restriction>
2367       </xs:complexContent>
2368     </xs:complexType>
2369
2370     <xs:complexType name="AuthenticatorBaseType">
2371       <xs:complexContent>
2372         <xs:restriction base="AuthenticatorBaseType">
2373           <xs:sequence>
2374             <xs:element ref="RestrictedPassword"/>
2375           </xs:sequence>
2376         </xs:restriction>
2377       </xs:complexContent>
2378     </xs:complexType>
2379
2380     <xs:complexType name="AuthenticatorTransportProtocolType">
2381       <xs:complexContent>
2382         <xs:restriction base="AuthenticatorTransportProtocolType">
2383           <xs:sequence>
2384             <xs:choice>
2385               <xs:element ref="SSL"/>
2386               <xs:element ref="MobileNetworkRadioEncryption"/>
2387               <xs:element ref="MobileNetworkEndToEndEncryption"/>
2388               <xs:element ref="WTLS"/>
2389               <xs:element ref="IPSec"/>
2390             </xs:choice>
2391             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2392           </xs:sequence>
2393         </xs:restriction>
2394       </xs:complexContent>
2395     </xs:complexType>
2396
2397   </xs:redefine>
2398
2399 </xs:schema>

```

2400 **3.4.10 PreviousSession**

2401 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession

2402 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2403 schema document [SAMLAC-Prev].

2404 The PreviousSession class is applicable when a principal had authenticated to an authentication authority
 2405 at some point in the past using any authentication context supported by that authentication authority.
 2406 Consequently, a subsequent authentication event that the authentication authority will assert to the relying
 2407 party may be significantly separated in time from the principal's current resource access request.

2408 The context for the previously authenticated session is explicitly not included in this context class because
 2409 the user has not authenticated during this session, and so the mechanism that the user employed to
 2410 authenticate in a previous session should not be used as part of a decision on whether to now allow
 2411 access to a resource.

```

2412 <?xml version="1.0" encoding="UTF-8"?>
2413

```

```

2414 <xs:schema
2415 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2416 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2417 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2418 finalDefault="extension"
2419 blockDefault="substitution"
2420 version="2.0">
2421
2422 <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2423
2424   <xs:annotation>
2425     <xs:documentation>
2426       Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
2427       Document identifier: saml-schema-authn-context-session-2.0
2428       Location: http://docs.oasis-open.org/security/saml/v2.0/
2429       Revision history:
2430         V2.0 (March, 2005):
2431         New authentication context class schema for SAML V2.0.
2432     </xs:documentation>
2433   </xs:annotation>
2434
2435   <xs:complexType name="AuthnContextDeclarationBaseType">
2436     <xs:complexContent>
2437       <xs:restriction base="AuthnContextDeclarationBaseType">
2438         <xs:sequence>
2439           <xs:element ref="Identification" minOccurs="0"/>
2440           <xs:element ref="TechnicalProtection" minOccurs="0"/>
2441           <xs:element ref="OperationalProtection" minOccurs="0"/>
2442           <xs:element ref="AuthnMethod"/>
2443           <xs:element ref="GoverningAgreements" minOccurs="0"/>
2444           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2445         </xs:sequence>
2446         <xs:attribute name="ID" type="xs:ID" use="optional"/>
2447       </xs:restriction>
2448     </xs:complexContent>
2449   </xs:complexType>
2450
2451   <xs:complexType name="AuthnMethodBaseType">
2452     <xs:complexContent>
2453       <xs:restriction base="AuthnMethodBaseType">
2454         <xs:sequence>
2455           <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
2456           <xs:element ref="Authenticator"/>
2457           <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2458           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2459         </xs:sequence>
2460       </xs:restriction>
2461     </xs:complexContent>
2462   </xs:complexType>
2463
2464   <xs:complexType name="AuthenticatorBaseType">
2465     <xs:complexContent>
2466       <xs:restriction base="AuthenticatorBaseType">
2467         <xs:sequence>
2468           <xs:element ref="PreviousSession"/>
2469         </xs:sequence>
2470       </xs:restriction>
2471     </xs:complexContent>
2472   </xs:complexType>
2473
2474 </xs:redefine>
2475
2476 </xs:schema>

```

2477 3.4.11 Public Key – X.509

2478 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:X509

2479 Note that this URI is also used as the target namespace in the corresponding authentication context class
2480 schema document [SAMLAC-X509].

2481 The X509 context class indicates that the principal authenticated by means of a digital signature where the
2482 key was validated as part of an X.509 Public Key Infrastructure.

```
2483 <?xml version="1.0" encoding="UTF-8"?>
2484
2485 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2486   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2487   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2488   finalDefault="extension"
2489   blockDefault="substitution"
2490   version="2.0">
2491
2492   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2493
2494     <xs:annotation>
2495       <xs:documentation>
2496         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:X509
2497         Document identifier: saml-schema-authn-context-x509-2.0
2498         Location: http://docs.oasis-open.org/security/saml/v2.0/
2499         Revision history:
2500           V2.0 (March, 2005):
2501             New authentication context class schema for SAML V2.0.
2502       </xs:documentation>
2503     </xs:annotation>
2504
2505     <xs:complexType name="AuthnContextDeclarationBaseType">
2506       <xs:complexContent>
2507         <xs:restriction base="AuthnContextDeclarationBaseType">
2508           <xs:sequence>
2509             <xs:element ref="Identification" minOccurs="0"/>
2510             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2511             <xs:element ref="OperationalProtection" minOccurs="0"/>
2512             <xs:element ref="AuthnMethod"/>
2513             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2514             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2515           </xs:sequence>
2516           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2517         </xs:restriction>
2518       </xs:complexContent>
2519     </xs:complexType>
2520
2521     <xs:complexType name="AuthnMethodBaseType">
2522       <xs:complexContent>
2523         <xs:restriction base="AuthnMethodBaseType">
2524           <xs:sequence>
2525             <xs:element ref="PrincipalAuthenticationMechanism"/>
2526             <xs:element ref="Authenticator"/>
2527             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2528             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2529           </xs:sequence>
2530         </xs:restriction>
2531       </xs:complexContent>
2532     </xs:complexType>
2533
2534     <xs:complexType name="PrincipalAuthenticationMechanismType">
2535       <xs:complexContent>
2536         <xs:restriction base="PrincipalAuthenticationMechanismType">
2537           <xs:sequence>
2538             <xs:element ref="RestrictedPassword"/>
```

```

2539         </xs:sequence>
2540         <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2541     </xs:restriction>
2542 </xs:complexContent>
2543 </xs:complexType>
2544
2545 <xs:complexType name="AuthenticatorBaseType">
2546 <xs:complexContent>
2547 <xs:restriction base="AuthenticatorBaseType">
2548 <xs:sequence>
2549 <xs:element ref="DigSig"/>
2550 </xs:sequence>
2551 </xs:restriction>
2552 </xs:complexContent>
2553 </xs:complexType>
2554
2555 <xs:complexType name="PublicKeyType">
2556 <xs:complexContent>
2557 <xs:restriction base="PublicKeyType">
2558 <xs:attribute name="keyValidation" type="xs:anyURI"
2559 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
2560 </xs:restriction>
2561 </xs:complexContent>
2562 </xs:complexType>
2563
2564 </xs:redefine>
2565
2566 </xs:schema>

```

2567 3.4.12 Public Key – PGP

2568 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PGP

2569 Note that this URI is also used as the target namespace in the corresponding authentication context class
2570 schema document [SAMLAC-PGP].

2571 The PGP context class indicates that the principal authenticated by means of a digital signature where the
2572 key was validated as part of a PGP Public Key Infrastructure.

```

2573 <?xml version="1.0" encoding="UTF-8"?>
2574
2575 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
2576 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2577 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
2578 finalDefault="extension"
2579 blockDefault="substitution"
2580 version="2.0">
2581
2582 <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2583
2584 <xs:annotation>
2585 <xs:documentation>
2586 Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
2587 Document identifier: saml-schema-authn-context-pgp-2.0
2588 Location: http://docs.oasis-open.org/security/saml/v2.0/
2589 Revision history:
2590 V2.0 (March, 2005):
2591 New authentication context class schema for SAML V2.0.
2592 </xs:documentation>
2593 </xs:annotation>
2594
2595 <xs:complexType name="AuthnContextDeclarationBaseType">
2596 <xs:complexContent>
2597 <xs:restriction base="AuthnContextDeclarationBaseType">
2598 <xs:sequence>
2599 <xs:element ref="Identification" minOccurs="0"/>

```

```

2600     <xs:element ref="TechnicalProtection" minOccurs="0"/>
2601     <xs:element ref="OperationalProtection" minOccurs="0"/>
2602     <xs:element ref="AuthnMethod"/>
2603     <xs:element ref="GoverningAgreements" minOccurs="0"/>
2604     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2605     </xs:sequence>
2606     <xs:attribute name="ID" type="xs:ID" use="optional"/>
2607   </xs:restriction>
2608 </xs:complexContent>
2609 </xs:complexType>
2610
2611 <xs:complexType name="AuthnMethodBaseType">
2612   <xs:complexContent>
2613     <xs:restriction base="AuthnMethodBaseType">
2614       <xs:sequence>
2615         <xs:element ref="PrincipalAuthenticationMechanism"/>
2616         <xs:element ref="Authenticator"/>
2617         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2618         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2619       </xs:sequence>
2620     </xs:restriction>
2621   </xs:complexContent>
2622 </xs:complexType>
2623
2624 <xs:complexType name="PrincipalAuthenticationMechanismType">
2625   <xs:complexContent>
2626     <xs:restriction base="PrincipalAuthenticationMechanismType">
2627       <xs:sequence>
2628         <xs:element ref="RestrictedPassword"/>
2629       </xs:sequence>
2630       <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2631     </xs:restriction>
2632   </xs:complexContent>
2633 </xs:complexType>
2634
2635 <xs:complexType name="AuthenticatorBaseType">
2636   <xs:complexContent>
2637     <xs:restriction base="AuthenticatorBaseType">
2638       <xs:sequence>
2639         <xs:element ref="DigSig"/>
2640       </xs:sequence>
2641     </xs:restriction>
2642   </xs:complexContent>
2643 </xs:complexType>
2644
2645 <xs:complexType name="PublicKeyType">
2646   <xs:complexContent>
2647     <xs:restriction base="PublicKeyType">
2648       <xs:attribute name="keyValidation"
2649 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
2650     </xs:restriction>
2651   </xs:complexContent>
2652 </xs:complexType>
2653
2654 </xs:redefine>
2655
2656 </xs:schema>

```

2657 3.4.13 Public Key – SPKI

2658 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI

2659 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2660 schema document [SAMLAC-SPKI].

2661 The SPKI context class indicates that the principal authenticated by means of a digital signature where the
2662 key was validated via an SPKI Infrastructure.

```
2663 <?xml version="1.0" encoding="UTF-8"?>
2664
2665 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2666   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2667   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2668   finalDefault="extension"
2669   blockDefault="substitution"
2670   version="2.0">
2671
2672   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2673
2674     <xs:annotation>
2675       <xs:documentation>
2676         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
2677         Document identifier: saml-schema-authn-context-spki-2.0
2678         Location: http://docs.oasis-open.org/security/saml/v2.0/
2679         Revision history:
2680           V2.0 (March, 2005):
2681             New authentication context class schema for SAML V2.0.
2682       </xs:documentation>
2683     </xs:annotation>
2684
2685     <xs:complexType name="AuthnContextDeclarationBaseType">
2686       <xs:complexContent>
2687         <xs:restriction base="AuthnContextDeclarationBaseType">
2688           <xs:sequence>
2689             <xs:element ref="Identification" minOccurs="0"/>
2690             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2691             <xs:element ref="OperationalProtection" minOccurs="0"/>
2692             <xs:element ref="AuthnMethod"/>
2693             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2694             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2695           </xs:sequence>
2696           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2697         </xs:restriction>
2698       </xs:complexContent>
2699     </xs:complexType>
2700
2701     <xs:complexType name="AuthnMethodBaseType">
2702       <xs:complexContent>
2703         <xs:restriction base="AuthnMethodBaseType">
2704           <xs:sequence>
2705             <xs:element ref="PrincipalAuthenticationMechanism"/>
2706             <xs:element ref="Authenticator"/>
2707             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2708             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2709           </xs:sequence>
2710         </xs:restriction>
2711       </xs:complexContent>
2712     </xs:complexType>
2713
2714     <xs:complexType name="PrincipalAuthenticationMechanismType">
2715       <xs:complexContent>
2716         <xs:restriction base="PrincipalAuthenticationMechanismType">
2717           <xs:sequence>
2718             <xs:element ref="RestrictedPassword"/>
2719           </xs:sequence>
2720           <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2721         </xs:restriction>
2722       </xs:complexContent>
2723     </xs:complexType>
2724
2725     <xs:complexType name="AuthenticatorBaseType">
2726       <xs:complexContent>
```

```

2727     <xs:restriction base="AuthenticatorBaseType">
2728         <xs:sequence>
2729             <xs:element ref="DigSig"/>
2730         </xs:sequence>
2731     </xs:restriction>
2732 </xs:complexContent>
2733 </xs:complexType>
2734
2735     <xs:complexType name="PublicKeyType">
2736         <xs:complexContent>
2737             <xs:restriction base="PublicKeyType">
2738                 <xs:attribute name="keyValidation"
2739 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
2740             </xs:restriction>
2741         </xs:complexContent>
2742     </xs:complexType>
2743
2744 </xs:redefine>
2745
2746 </xs:schema>

```

2747 3.4.14 Public Key - XML Digital Signature

2748 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig

2749 Note that this URI is also used as the target namespace in the corresponding authentication context class
2750 schema document [SAMLAC-XSig]

2751 This context class indicates that the principal authenticated by means of a digital signature according to
2752 the processing rules specified in the XML Digital Signature specification [XMLSig].

```

2753 <?xml version="1.0" encoding="UTF-8"?>
2754
2755 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
2756 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2757 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
2758 finalDefault="extension"
2759 blockDefault="substitution"
2760 version="2.0">
2761
2762 <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2763
2764     <xs:annotation>
2765         <xs:documentation>
2766             Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
2767             Document identifier: saml-schema-authn-context-xmldsig-2.0
2768             Location: http://docs.oasis-open.org/security/saml/v2.0/
2769             Revision history:
2770                 V2.0 (March, 2005):
2771                 New authentication context class schema for SAML V2.0.
2772         </xs:documentation>
2773     </xs:annotation>
2774
2775     <xs:complexType name="AuthnContextDeclarationBaseType">
2776         <xs:complexContent>
2777             <xs:restriction base="AuthnContextDeclarationBaseType">
2778                 <xs:sequence>
2779                     <xs:element ref="Identification" minOccurs="0"/>
2780                     <xs:element ref="TechnicalProtection" minOccurs="0"/>
2781                     <xs:element ref="OperationalProtection" minOccurs="0"/>
2782                     <xs:element ref="AuthnMethod"/>
2783                     <xs:element ref="GoverningAgreements" minOccurs="0"/>
2784                     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2785                 </xs:sequence>
2786                 <xs:attribute name="ID" type="xs:ID" use="optional"/>
2787             </xs:restriction>

```



```

2788     </xs:complexContent>
2789 </xs:complexType>
2790
2791 <xs:complexType name="AuthnMethodBaseType">
2792   <xs:complexContent>
2793     <xs:restriction base="AuthnMethodBaseType">
2794       <xs:sequence>
2795         <xs:element ref="PrincipalAuthenticationMechanism"/>
2796         <xs:element ref="Authenticator"/>
2797         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2798         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2799       </xs:sequence>
2800     </xs:restriction>
2801   </xs:complexContent>
2802 </xs:complexType>
2803
2804 <xs:complexType name="PrincipalAuthenticationMechanismType">
2805   <xs:complexContent>
2806     <xs:restriction base="PrincipalAuthenticationMechanismType">
2807       <xs:sequence>
2808         <xs:element ref="RestrictedPassword"/>
2809       </xs:sequence>
2810       <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2811     </xs:restriction>
2812   </xs:complexContent>
2813 </xs:complexType>
2814
2815 <xs:complexType name="AuthenticatorBaseType">
2816   <xs:complexContent>
2817     <xs:restriction base="AuthenticatorBaseType">
2818       <xs:sequence>
2819         <xs:element ref="DigSig"/>
2820       </xs:sequence>
2821     </xs:restriction>
2822   </xs:complexContent>
2823 </xs:complexType>
2824
2825 <xs:complexType name="PublicKeyType">
2826   <xs:complexContent>
2827     <xs:restriction base="PublicKeyType">
2828       <xs:attribute name="keyValidation" type="xs:anyURI"
2829 fixed="urn:ietf:rfc:3075"/>
2830     </xs:restriction>
2831   </xs:complexContent>
2832 </xs:complexType>
2833
2834 </xs:redefine>
2835
2836 </xs:schema>

```

2837 3.4.15 Smartcard

2838 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard

2839 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2840 schema document [SAMLAC-Smart].

2841 The Smartcard class is identified when a principal authenticates to an authentication authority using a
 2842 smartcard.

```

2843 <?xml version="1.0" encoding="UTF-8"?>
2844
2845 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
2846   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2847   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
2848   finalDefault="extension"

```

```

2849 blockDefault="substitution"
2850 version="2.0">
2851
2852 <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2853
2854   <xs:annotation>
2855     <xs:documentation>
2856       Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
2857       Document identifier: saml-schema-authn-context-smartcard-2.0
2858       Location: http://docs.oasis-open.org/security/saml/v2.0/
2859       Revision history:
2860         V2.0 (March, 2005):
2861         New authentication context class schema for SAML V2.0.
2862     </xs:documentation>
2863   </xs:annotation>
2864
2865   <xs:complexType name="AuthnContextDeclarationBaseType">
2866     <xs:complexContent>
2867       <xs:restriction base="AuthnContextDeclarationBaseType">
2868         <xs:sequence>
2869           <xs:element ref="Identification" minOccurs="0"/>
2870           <xs:element ref="TechnicalProtection" minOccurs="0"/>
2871           <xs:element ref="OperationalProtection" minOccurs="0"/>
2872           <xs:element ref="AuthnMethod"/>
2873           <xs:element ref="GoverningAgreements" minOccurs="0"/>
2874           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2875         </xs:sequence>
2876         <xs:attribute name="ID" type="xs:ID" use="optional"/>
2877       </xs:restriction>
2878     </xs:complexContent>
2879   </xs:complexType>
2880
2881   <xs:complexType name="AuthnMethodBaseType">
2882     <xs:complexContent>
2883       <xs:restriction base="AuthnMethodBaseType">
2884         <xs:sequence>
2885           <xs:element ref="PrincipalAuthenticationMechanism"/>
2886           <xs:element ref="Authenticator"/>
2887           <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2888           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2889         </xs:sequence>
2890       </xs:restriction>
2891     </xs:complexContent>
2892   </xs:complexType>
2893
2894   <xs:complexType name="PrincipalAuthenticationMechanismType">
2895     <xs:complexContent>
2896       <xs:restriction base="PrincipalAuthenticationMechanismType">
2897         <xs:sequence>
2898           <xs:element ref="Smartcard"/>
2899         </xs:sequence>
2900       </xs:restriction>
2901     </xs:complexContent>
2902   </xs:complexType>
2903
2904 </xs:redefine>
2905
2906 </xs:schema>

```

2907 **3.4.16 SmartcardPKI**

2908 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

2909 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2910 schema document [SAMLAC-SmPKI].

2911 The SmartcardPKI class is applicable when a principal authenticates to an authentication authority through
2912 a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN.

```
2913 <?xml version="1.0" encoding="UTF-8"?>
2914
2915 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
2916   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2917   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
2918   finalDefault="extension"
2919   blockDefault="substitution"
2920   version="2.0">
2921
2922   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
2923
2924     <xs:annotation>
2925       <xs:documentation>
2926         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
2927         Document identifier: saml-schema-authn-context-smartcardpki-2.0
2928         Location: http://docs.oasis-open.org/security/saml/v2.0/
2929         Revision history:
2930           V2.0 (March, 2005):
2931           New authentication context class schema for SAML V2.0.
2932       </xs:documentation>
2933     </xs:annotation>
2934
2935     <xs:complexType name="AuthnContextDeclarationBaseType">
2936       <xs:complexContent>
2937         <xs:restriction base="AuthnContextDeclarationBaseType">
2938           <xs:sequence>
2939             <xs:element ref="Identification" minOccurs="0"/>
2940             <xs:element ref="TechnicalProtection"/>
2941             <xs:element ref="OperationalProtection" minOccurs="0"/>
2942             <xs:element ref="AuthnMethod"/>
2943             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2944             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2945           </xs:sequence>
2946           <xs:attribute name="ID" type="xs:ID" use="optional"/>
2947         </xs:restriction>
2948       </xs:complexContent>
2949     </xs:complexType>
2950
2951     <xs:complexType name="AuthnMethodBaseType">
2952       <xs:complexContent>
2953         <xs:restriction base="AuthnMethodBaseType">
2954           <xs:sequence>
2955             <xs:element ref="PrincipalAuthenticationMechanism"/>
2956             <xs:element ref="Authenticator"/>
2957             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
2958             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2959           </xs:sequence>
2960         </xs:restriction>
2961       </xs:complexContent>
2962     </xs:complexType>
2963
2964     <xs:complexType name="TechnicalProtectionBaseType">
2965       <xs:complexContent>
2966         <xs:restriction base="TechnicalProtectionBaseType">
2967           <xs:sequence>
2968             <xs:choice>
2969               <xs:element ref="PrivateKeyProtection"/>
2970             </xs:choice>
2971           </xs:sequence>
2972         </xs:restriction>
2973       </xs:complexContent>
2974     </xs:complexType>
2975
2976     <xs:complexType name="PrincipalAuthenticationMechanismType">
```

```

2977     <xs:complexContent>
2978     <xs:restriction base="PrincipalAuthenticationMechanismType">
2979         <xs:sequence>
2980             <xs:element ref="Smartcard"/>
2981             <xs:element ref="ActivationPin"/>
2982             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2983         </xs:sequence>
2984     </xs:restriction>
2985 </xs:complexContent>
2986 </xs:complexType>
2987
2988 <xs:complexType name="AuthenticatorBaseType">
2989     <xs:complexContent>
2990     <xs:restriction base="AuthenticatorBaseType">
2991         <xs:sequence>
2992             <xs:choice>
2993                 <xs:element ref="DigSig"/>
2994                 <xs:element ref="AsymmetricDecryption"/>
2995                 <xs:element ref="AsymmetricKeyAgreement"/>
2996             </xs:choice>
2997             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
2998         </xs:sequence>
2999     </xs:restriction>
3000 </xs:complexContent>
3001 </xs:complexType>
3002
3003 <xs:complexType name="PrivateKeyProtectionType">
3004     <xs:complexContent>
3005     <xs:restriction base="PrivateKeyProtectionType">
3006         <xs:sequence>
3007             <xs:element ref="KeyActivation"/>
3008             <xs:element ref="KeyStorage"/>
3009             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3010         </xs:sequence>
3011     </xs:restriction>
3012 </xs:complexContent>
3013 </xs:complexType>
3014
3015 <xs:complexType name="KeyActivationType">
3016     <xs:complexContent>
3017     <xs:restriction base="KeyActivationType">
3018         <xs:sequence>
3019             <xs:element ref="ActivationPin"/>
3020         </xs:sequence>
3021     </xs:restriction>
3022 </xs:complexContent>
3023 </xs:complexType>
3024
3025 <xs:complexType name="KeyStorageType">
3026     <xs:complexContent>
3027     <xs:restriction base="KeyStorageType">
3028         <xs:attribute name="medium" use="required">
3029             <xs:simpleType>
3030                 <xs:restriction base="mediumType">
3031                     <xs:enumeration value="smartcard"/>
3032                 </xs:restriction>
3033             </xs:simpleType>
3034         </xs:attribute>
3035     </xs:restriction>
3036 </xs:complexContent>
3037 </xs:complexType>
3038
3039 </xs:redefine>
3040
3041 </xs:schema>

```

3042 3.4.17 SoftwarePKI

3043 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI

3044 Note that this URI is also used as the target namespace in the corresponding authentication context class
3045 schema document [SAMLAC-SwPKI] .

3046 The Software-PKI class is applicable when a principal uses an X.509 certificate stored in software to
3047 authenticate to the authentication authority.

```
3048 <?xml version="1.0" encoding="UTF-8"?>
3049
3050 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3051   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3052   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3053   finalDefault="extension"
3054   blockDefault="substitution"
3055   version="2.0">
3056
3057   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
3058
3059     <xs:annotation>
3060       <xs:documentation>
3061         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
3062         Document identifier: saml-schema-authn-context-softwarepki-2.0
3063         Location: http://docs.oasis-open.org/security/saml/v2.0/
3064         Revision history:
3065           V2.0 (March, 2005):
3066             New authentication context class schema for SAML V2.0.
3067       </xs:documentation>
3068     </xs:annotation>
3069
3070     <xs:complexType name="AuthnContextDeclarationBaseType">
3071       <xs:complexContent>
3072         <xs:restriction base="AuthnContextDeclarationBaseType">
3073           <xs:sequence>
3074             <xs:element ref="Identification" minOccurs="0"/>
3075             <xs:element ref="TechnicalProtection"/>
3076             <xs:element ref="OperationalProtection" minOccurs="0"/>
3077             <xs:element ref="AuthnMethod"/>
3078             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3079             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3080           </xs:sequence>
3081           <xs:attribute name="ID" type="xs:ID" use="optional"/>
3082         </xs:restriction>
3083       </xs:complexContent>
3084     </xs:complexType>
3085
3086     <xs:complexType name="AuthnMethodBaseType">
3087       <xs:complexContent>
3088         <xs:restriction base="AuthnMethodBaseType">
3089           <xs:sequence>
3090             <xs:element ref="PrincipalAuthenticationMechanism"/>
3091             <xs:element ref="Authenticator"/>
3092             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
3093             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3094           </xs:sequence>
3095         </xs:restriction>
3096       </xs:complexContent>
3097     </xs:complexType>
3098
3099     <xs:complexType name="TechnicalProtectionBaseType">
3100       <xs:complexContent>
3101         <xs:restriction base="TechnicalProtectionBaseType">
3102           <xs:sequence>
3103             <xs:choice>
```

```

3104         <xs:element ref="PrivateKeyProtection"/>
3105     </xs:choice>
3106 </xs:sequence>
3107 </xs:restriction>
3108 </xs:complexContent>
3109 </xs:complexType>
3110
3111 <xs:complexType name="PrincipalAuthenticationMechanismType">
3112     <xs:complexContent>
3113         <xs:restriction base="PrincipalAuthenticationMechanismType">
3114             <xs:sequence>
3115                 <xs:element ref="ActivationPin"/>
3116                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3117             </xs:sequence>
3118         </xs:restriction>
3119     </xs:complexContent>
3120 </xs:complexType>
3121
3122 <xs:complexType name="AuthenticatorBaseType">
3123     <xs:complexContent>
3124         <xs:restriction base="AuthenticatorBaseType">
3125             <xs:sequence>
3126                 <xs:choice>
3127                     <xs:element ref="DigSig"/>
3128                     <xs:element ref="AsymmetricDecryption"/>
3129                     <xs:element ref="AsymmetricKeyAgreement"/>
3130                 </xs:choice>
3131                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3132             </xs:sequence>
3133         </xs:restriction>
3134     </xs:complexContent>
3135 </xs:complexType>
3136
3137 <xs:complexType name="PrivateKeyProtectionType">
3138     <xs:complexContent>
3139         <xs:restriction base="PrivateKeyProtectionType">
3140             <xs:sequence>
3141                 <xs:element ref="KeyActivation"/>
3142                 <xs:element ref="KeyStorage"/>
3143                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3144             </xs:sequence>
3145         </xs:restriction>
3146     </xs:complexContent>
3147 </xs:complexType>
3148
3149 <xs:complexType name="KeyActivationType">
3150     <xs:complexContent>
3151         <xs:restriction base="KeyActivationType">
3152             <xs:sequence>
3153                 <xs:element ref="ActivationPin"/>
3154                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3155             </xs:sequence>
3156         </xs:restriction>
3157     </xs:complexContent>
3158 </xs:complexType>
3159
3160 <xs:complexType name="KeyStorageType">
3161     <xs:complexContent>
3162         <xs:restriction base="KeyStorageType">
3163             <xs:attribute name="medium" use="required">
3164                 <xs:simpleType>
3165                     <xs:restriction base="mediumType">
3166                         <xs:enumeration value="memory"/>
3167                     </xs:restriction>
3168                 </xs:simpleType>
3169             </xs:attribute>
3170         </xs:restriction>

```

```
3171     </xs:complexContent>
3172     </xs:complexType>
3173
3174     </xs:redefine>
3175 </xs:schema>
```

3176 3.4.18 Telephony

3177 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony

3178 Note that this URI is also used as the target namespace in the corresponding authentication context class
3179 schema document [SAMLAC-Tele].

3180 This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone
3181 number, transported via a telephony protocol such as ADSL.

```
3182 <?xml version="1.0" encoding="UTF-8"?>
3183
3184 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3185   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3186   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3187   finalDefault="extension"
3188   blockDefault="substitution"
3189   version="2.0">
3190
3191   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
3192
3193     <xs:annotation>
3194       <xs:documentation>
3195         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
3196         Document identifier: saml-schema-authn-context-telephony-2.0
3197         Location: http://docs.oasis-open.org/security/saml/v2.0/
3198         Revision history:
3199           V2.0 (March, 2005):
3200             New authentication context class schema for SAML V2.0.
3201       </xs:documentation>
3202     </xs:annotation>
3203
3204     <xs:complexType name="AuthnContextDeclarationBaseType">
3205       <xs:complexContent>
3206         <xs:restriction base="AuthnContextDeclarationBaseType">
3207           <xs:sequence>
3208             <xs:element ref="Identification" minOccurs="0"/>
3209             <xs:element ref="TechnicalProtection" minOccurs="0"/>
3210             <xs:element ref="OperationalProtection" minOccurs="0"/>
3211             <xs:element ref="AuthnMethod"/>
3212             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3213             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3214           </xs:sequence>
3215           <xs:attribute name="ID" type="xs:ID" use="optional"/>
3216         </xs:restriction>
3217       </xs:complexContent>
3218     </xs:complexType>
3219
3220     <xs:complexType name="AuthnMethodBaseType">
3221       <xs:complexContent>
3222         <xs:restriction base="AuthnMethodBaseType">
3223           <xs:sequence>
3224             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3225             <xs:element ref="Authenticator"/>
3226             <xs:element ref="AuthenticatorTransportProtocol"/>
3227             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3228           </xs:sequence>
3229         </xs:restriction>
3230       </xs:complexContent>
3231     </xs:complexType>
```

```

3232
3233     <xs:complexType name="AuthenticatorBaseType">
3234       <xs:complexContent>
3235         <xs:restriction base="AuthenticatorBaseType">
3236           <xs:sequence>
3237             <xs:element ref="SubscriberLineNumber"/>
3238           </xs:sequence>
3239         </xs:restriction>
3240       </xs:complexContent>
3241     </xs:complexType>
3242
3243     <xs:complexType name="AuthenticatorTransportProtocolType">
3244       <xs:complexContent>
3245         <xs:restriction base="AuthenticatorTransportProtocolType">
3246           <xs:sequence>
3247             <xs:choice>
3248               <xs:element ref="PSTN"/>
3249               <xs:element ref="ISDN"/>
3250               <xs:element ref="ADSL"/>
3251             </xs:choice>
3252             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3253           </xs:sequence>
3254         </xs:restriction>
3255       </xs:complexContent>
3256     </xs:complexType>
3257
3258   </xs:redefine>
3259
3260 </xs:schema>

```

3261 3.4.19 Telephony ("Nomadic")

3262 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony

3263 Note that this URI is also used as the target namespace in the corresponding authentication context class
3264 schema document [SAMLAC-TNom].

3265 Indicates that the principal is "roaming" (perhaps using a phone card) and authenticates via the means of
3266 the line number, a user suffix, and a password element.

```

3267 <?xml version="1.0" encoding="UTF-8"?>
3268
3269 <xs:schema
3270 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3271 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3272 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3273 finalDefault="extension"
3274 blockDefault="substitution"
3275 version="2.0">
3276
3277   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
3278
3279     <xs:annotation>
3280       <xs:documentation>
3281         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
3282         Document identifier: saml-schema-authn-context-nomad-telephony-2.0
3283         Location: http://docs.oasis-open.org/security/saml/v2.0/
3284         Revision history:
3285           V2.0 (March, 2005):
3286             New authentication context class schema for SAML V2.0.
3287       </xs:documentation>
3288     </xs:annotation>
3289
3290     <xs:complexType name="AuthnContextDeclarationBaseType">
3291       <xs:complexContent>
3292         <xs:restriction base="AuthnContextDeclarationBaseType">

```



```

3293     <xs:sequence>
3294         <xs:element ref="Identification" minOccurs="0"/>
3295         <xs:element ref="TechnicalProtection" minOccurs="0"/>
3296         <xs:element ref="OperationalProtection" minOccurs="0"/>
3297         <xs:element ref="AuthnMethod"/>
3298         <xs:element ref="GoverningAgreements" minOccurs="0"/>
3299         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3300     </xs:sequence>
3301     <xs:attribute name="ID" type="xs:ID" use="optional"/>
3302 </xs:restriction>
3303 </xs:complexContent>
3304 </xs:complexType>
3305
3306 <xs:complexType name="AuthnMethodBaseType">
3307     <xs:complexContent>
3308         <xs:restriction base="AuthnMethodBaseType">
3309             <xs:sequence>
3310                 <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3311                 <xs:element ref="Authenticator"/>
3312                 <xs:element ref="AuthenticatorTransportProtocol"/>
3313                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3314             </xs:sequence>
3315         </xs:restriction>
3316     </xs:complexContent>
3317 </xs:complexType>
3318
3319 <xs:complexType name="AuthenticatorBaseType">
3320     <xs:complexContent>
3321         <xs:restriction base="AuthenticatorBaseType">
3322             <xs:sequence>
3323                 <xs:element ref="Password"/>
3324                 <xs:element ref="SubscriberLineNumber"/>
3325                 <xs:element ref="UserSuffix"/>
3326             </xs:sequence>
3327         </xs:restriction>
3328     </xs:complexContent>
3329 </xs:complexType>
3330
3331 <xs:complexType name="AuthenticatorTransportProtocolType">
3332     <xs:complexContent>
3333         <xs:restriction base="AuthenticatorTransportProtocolType">
3334             <xs:sequence>
3335                 <xs:choice>
3336                     <xs:element ref="PSTN"/>
3337                     <xs:element ref="ISDN"/>
3338                     <xs:element ref="ADSL"/>
3339                 </xs:choice>
3340                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3341             </xs:sequence>
3342         </xs:restriction>
3343     </xs:complexContent>
3344 </xs:complexType>
3345
3346 </xs:redefine>
3347
3348 </xs:schema>

```

3349 **3.4.20 Telephony (Personalized)**

3350 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony

3351 Note that this URI is also used as the target namespace in the corresponding authentication context class
3352 schema document [SAMLAC-TPers].

3353 This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone
3354 number and a user suffix, transported via a telephony protocol such as ADSL.

```

3355 <?xml version="1.0" encoding="UTF-8"?>
3356
3357 <xs:schema
3358 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
3359 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3360 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
3361 finalDefault="extension"
3362 blockDefault="substitution"
3363 version="2.0">
3364
3365 <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
3366
3367 <xs:annotation>
3368 <xs:documentation>
3369 Class identifier:
3370 urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony
3371 Document identifier: saml-schema-authn-context-personal-telephony-2.0
3372 Location: http://docs.oasis-open.org/security/saml/v2.0/
3373 Revision history:
3374 V2.0 (March, 2005):
3375 New authentication context class schema for SAML V2.0.
3376 </xs:documentation>
3377 </xs:annotation>
3378
3379 <xs:complexType name="AuthnContextDeclarationBaseType">
3380 <xs:complexContent>
3381 <xs:restriction base="AuthnContextDeclarationBaseType">
3382 <xs:sequence>
3383 <xs:element ref="Identification" minOccurs="0"/>
3384 <xs:element ref="TechnicalProtection" minOccurs="0"/>
3385 <xs:element ref="OperationalProtection" minOccurs="0"/>
3386 <xs:element ref="AuthnMethod"/>
3387 <xs:element ref="GoverningAgreements" minOccurs="0"/>
3388 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3389 </xs:sequence>
3390 <xs:attribute name="ID" type="xs:ID" use="optional"/>
3391 </xs:restriction>
3392 </xs:complexContent>
3393 </xs:complexType>
3394
3395 <xs:complexType name="AuthnMethodBaseType">
3396 <xs:complexContent>
3397 <xs:restriction base="AuthnMethodBaseType">
3398 <xs:sequence>
3399 <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3400 <xs:element ref="Authenticator"/>
3401 <xs:element ref="AuthenticatorTransportProtocol"/>
3402 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3403 </xs:sequence>
3404 </xs:restriction>
3405 </xs:complexContent>
3406 </xs:complexType>
3407
3408 <xs:complexType name="AuthenticatorBaseType">
3409 <xs:complexContent>
3410 <xs:restriction base="AuthenticatorBaseType">
3411 <xs:sequence>
3412 <xs:element ref="SubscriberLineNumber"/>
3413 <xs:element ref="UserSuffix"/>
3414 </xs:sequence>
3415 </xs:restriction>
3416 </xs:complexContent>
3417 </xs:complexType>
3418
3419 <xs:complexType name="AuthenticatorTransportProtocolType">
3420 <xs:complexContent>
3421 <xs:restriction base="AuthenticatorTransportProtocolType">

```

```

3422     <xs:sequence>
3423         <xs:choice>
3424             <xs:element ref="PSTN"/>
3425             <xs:element ref="ISDN"/>
3426             <xs:element ref="ADSL"/>
3427         </xs:choice>
3428         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3429     </xs:sequence>
3430 </xs:restriction>
3431 </xs:complexContent>
3432 </xs:complexType>
3433
3434 </xs:redefine>
3435
3436 </xs:schema>

```

3437 3.4.21 Telephony (Authenticated)

3438 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony

3439 Note that this URI is also used as the target namespace in the corresponding authentication context class
3440 schema document [SAMLAC-TAuthn].

3441 Indicates that the principal authenticated via the means of the line number, a user suffix, and a password
3442 element.

```

3443 <?xml version="1.0" encoding="UTF-8"?>
3444
3445 <xs:schema
3446 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3447 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3448 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3449 finalDefault="extension"
3450 blockDefault="substitution"
3451 version="2.0">
3452
3453   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
3454
3455     <xs:annotation>
3456       <xs:documentation>
3457         Class identifier:
3458 urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
3459         Document identifier: saml-schema-authn-context-auth-telephony-2.0
3460         Location: http://docs.oasis-open.org/security/saml/v2.0/
3461         Revision history:
3462           V2.0 (March, 2005):
3463             New authentication context class schema for SAML V2.0.
3464       </xs:documentation>
3465     </xs:annotation>
3466
3467     <xs:complexType name="AuthnContextDeclarationBaseType">
3468       <xs:complexContent>
3469         <xs:restriction base="AuthnContextDeclarationBaseType">
3470           <xs:sequence>
3471             <xs:element ref="Identification" minOccurs="0"/>
3472             <xs:element ref="TechnicalProtection" minOccurs="0"/>
3473             <xs:element ref="OperationalProtection" minOccurs="0"/>
3474             <xs:element ref="AuthnMethod"/>
3475             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3476             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3477           </xs:sequence>
3478           <xs:attribute name="ID" type="xs:ID" use="optional"/>
3479         </xs:restriction>
3480       </xs:complexContent>
3481     </xs:complexType>
3482

```

```

3483     <xs:complexType name="AuthnMethodBaseType">
3484       <xs:complexContent>
3485         <xs:restriction base="AuthnMethodBaseType">
3486           <xs:sequence>
3487             <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3488             <xs:element ref="Authenticator"/>
3489             <xs:element ref="AuthenticatorTransportProtocol"/>
3490             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3491           </xs:sequence>
3492         </xs:restriction>
3493       </xs:complexContent>
3494     </xs:complexType>
3495
3496     <xs:complexType name="AuthenticatorBaseType">
3497       <xs:complexContent>
3498         <xs:restriction base="AuthenticatorBaseType">
3499           <xs:sequence>
3500             <xs:element ref="Password"/>
3501             <xs:element ref="SubscriberLineNumber"/>
3502             <xs:element ref="UserSuffix"/>
3503           </xs:sequence>
3504         </xs:restriction>
3505       </xs:complexContent>
3506     </xs:complexType>
3507
3508     <xs:complexType name="AuthenticatorTransportProtocolType">
3509       <xs:complexContent>
3510         <xs:restriction base="AuthenticatorTransportProtocolType">
3511           <xs:sequence>
3512             <xs:choice>
3513               <xs:element ref="PSTN"/>
3514               <xs:element ref="ISDN"/>
3515               <xs:element ref="ADSL"/>
3516             </xs:choice>
3517             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3518           </xs:sequence>
3519         </xs:restriction>
3520       </xs:complexContent>
3521     </xs:complexType>
3522   </xs:redefine>
3523 </xs:schema>
3524

```

3525 3.4.22 Secure Remote Password

3526 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword

3527 Note that this URI is also used as the target namespace in the corresponding authentication context class
3528 schema document [SAMLAC-SRP].

3529 The Secure Remote Password class is applicable when the authentication was performed by means of
3530 Secure Remote Password as specified in [RFC 2945].

```

3531 <?xml version="1.0" encoding="UTF-8"?>
3532
3533 <xs:schema
3534   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
3535   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3536   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
3537   finalDefault="extension"
3538   blockDefault="substitution"
3539   version="2.0">
3540
3541   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
3542
3543     <xs:annotation>

```

```

3544     <xs:documentation>
3545         Class identifier:
3546         urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
3547         Document identifier: saml-schema-authn-context-srp-2.0
3548         Location: http://docs.oasis-open.org/security/saml/v2.0/
3549         Revision history:
3550             V2.0 (March, 2005):
3551             New authentication context class schema for SAML V2.0.
3552     </xs:documentation>
3553 </xs:annotation>
3554
3555 <xs:complexType name="AuthnContextDeclarationBaseType">
3556     <xs:complexContent>
3557         <xs:restriction base="AuthnContextDeclarationBaseType">
3558             <xs:sequence>
3559                 <xs:element ref="Identification" minOccurs="0"/>
3560                 <xs:element ref="TechnicalProtection" minOccurs="0"/>
3561                 <xs:element ref="OperationalProtection" minOccurs="0"/>
3562                 <xs:element ref="AuthnMethod"/>
3563                 <xs:element ref="GoverningAgreements" minOccurs="0"/>
3564                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3565             </xs:sequence>
3566             <xs:attribute name="ID" type="xs:ID" use="optional"/>
3567         </xs:restriction>
3568     </xs:complexContent>
3569 </xs:complexType>
3570
3571 <xs:complexType name="AuthnMethodBaseType">
3572     <xs:complexContent>
3573         <xs:restriction base="AuthnMethodBaseType">
3574             <xs:sequence>
3575                 <xs:element ref="PrincipalAuthenticationMechanism"/>
3576                 <xs:element ref="Authenticator"/>
3577                 <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
3578                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3579             </xs:sequence>
3580         </xs:restriction>
3581     </xs:complexContent>
3582 </xs:complexType>
3583
3584 <xs:complexType name="PrincipalAuthenticationMechanismType">
3585     <xs:complexContent>
3586         <xs:restriction base="PrincipalAuthenticationMechanismType">
3587             <xs:sequence>
3588                 <xs:element ref="RestrictedPassword"/>
3589             </xs:sequence>
3590         </xs:restriction>
3591     </xs:complexContent>
3592 </xs:complexType>
3593
3594 <xs:complexType name="AuthenticatorBaseType">
3595     <xs:complexContent>
3596         <xs:restriction base="AuthenticatorBaseType">
3597             <xs:sequence>
3598                 <xs:element ref="SharedSecretChallengeResponse"/>
3599             </xs:sequence>
3600         </xs:restriction>
3601     </xs:complexContent>
3602 </xs:complexType>
3603
3604 <xs:complexType name="SharedSecretChallengeResponseType">
3605     <xs:complexContent>
3606         <xs:restriction base="SharedSecretChallengeResponseType">
3607             <xs:attribute name="method" type="xs:anyURI"
3608 fixed="urn:ietf:rfc:2945"/>
3609         </xs:restriction>
3610     </xs:complexContent>

```

```
3611     </xs:complexType>
3612
3613     </xs:redefine>
3614
3615 </xs:schema>
```

3616 3.4.23 SSL/TLS Certificate-Based Client Authentication

3617 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient

3618 Note that this URI is also used as the target namespace in the corresponding authentication context class
3619 schema document [SAMLAC-SSL].

3620 This class indicates that the principal authenticated by means of a client certificate, secured with the
3621 SSL/TLS transport.

```
3622 <?xml version="1.0" encoding="UTF-8"?>
3623
3624 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
3625   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3626   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
3627   finalDefault="extension"
3628   blockDefault="substitution"
3629   version="2.0">
3630
3631   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
3632
3633     <xs:annotation>
3634       <xs:documentation>
3635         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
3636         Document identifier: saml-schema-authn-context-sslcert-2.0
3637         Location: http://docs.oasis-open.org/security/saml/v2.0/
3638         Revision history:
3639           V2.0 (March, 2005):
3640             New authentication context class schema for SAML V2.0.
3641       </xs:documentation>
3642     </xs:annotation>
3643
3644     <xs:complexType name="AuthnContextDeclarationBaseType">
3645       <xs:complexContent>
3646         <xs:restriction base="AuthnContextDeclarationBaseType">
3647           <xs:sequence>
3648             <xs:element ref="Identification" minOccurs="0"/>
3649             <xs:element ref="TechnicalProtection" minOccurs="0"/>
3650             <xs:element ref="OperationalProtection" minOccurs="0"/>
3651             <xs:element ref="AuthnMethod"/>
3652             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3653             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3654           </xs:sequence>
3655           <xs:attribute name="ID" type="xs:ID" use="optional"/>
3656         </xs:restriction>
3657       </xs:complexContent>
3658     </xs:complexType>
3659
3660     <xs:complexType name="AuthnMethodBaseType">
3661       <xs:complexContent>
3662         <xs:restriction base="AuthnMethodBaseType">
3663           <xs:sequence>
3664             <xs:element ref="PrincipalAuthenticationMechanism"/>
3665             <xs:element ref="Authenticator"/>
3666             <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
3667             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3668           </xs:sequence>
3669         </xs:restriction>
3670       </xs:complexContent>
3671     </xs:complexType>
```

```

3672
3673     <xs:complexType name="PrincipalAuthenticationMechanismType">
3674     <xs:complexContent>
3675     <xs:restriction base="PrincipalAuthenticationMechanismType">
3676     <xs:sequence>
3677     <xs:element ref="RestrictedPassword"/>
3678     </xs:sequence>
3679     <xs:attribute name="preauth" type="xs:integer" use="optional"/>
3680     </xs:restriction>
3681     </xs:complexContent>
3682     </xs:complexType>
3683
3684     <xs:complexType name="AuthenticatorBaseType">
3685     <xs:complexContent>
3686     <xs:restriction base="AuthenticatorBaseType">
3687     <xs:sequence>
3688     <xs:element ref="DigSig"/>
3689     </xs:sequence>
3690     </xs:restriction>
3691     </xs:complexContent>
3692     </xs:complexType>
3693
3694     <xs:complexType name="PublicKeyType">
3695     <xs:complexContent>
3696     <xs:restriction base="PublicKeyType">
3697     <xs:attribute name="keyValidation" type="xs:anyURI"
3698     fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
3699     </xs:restriction>
3700     </xs:complexContent>
3701     </xs:complexType>
3702
3703     <xs:complexType name="AuthenticatorTransportProtocolType">
3704     <xs:complexContent>
3705     <xs:restriction base="AuthenticatorTransportProtocolType">
3706     <xs:sequence>
3707     <xs:choice>
3708     <xs:element ref="SSL"/>
3709     <xs:element ref="WTLS"/>
3710     </xs:choice>
3711     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3712     </xs:sequence>
3713     </xs:restriction>
3714     </xs:complexContent>
3715     </xs:complexType>
3716
3717     </xs:redefine>
3718
3719 </xs:schema>

```

3720 3.4.24 TimeSyncToken

3721 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken

3722 Note that this URI is also used as the target namespace in the corresponding authentication context class
3723 schema document [SAMLAC-TST].

3724 The TimeSyncToken class is applicable when a principal authenticates through a time synchronization
3725 token.

```

3726 <?xml version="1.0" encoding="UTF-8"?>
3727
3728 <xs:schema
3729 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
3730 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3731 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
3732 finalDefault="extension"

```

```

3733 blockDefault="substitution"
3734 version="2.0">
3735
3736 <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
3737
3738   <xs:annotation>
3739     <xs:documentation>
3740       Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
3741       Document identifier: saml-schema-authn-context-timesync-2.0
3742       Location: http://docs.oasis-open.org/security/saml/v2.0/
3743       Revision history:
3744         V2.0 (March, 2005):
3745         New authentication context class schema for SAML V2.0.
3746     </xs:documentation>
3747   </xs:annotation>
3748
3749   <xs:complexType name="AuthnContextDeclarationBaseType">
3750     <xs:complexContent>
3751       <xs:restriction base="AuthnContextDeclarationBaseType">
3752         <xs:sequence>
3753           <xs:element ref="Identification" minOccurs="0"/>
3754           <xs:element ref="TechnicalProtection" minOccurs="0"/>
3755           <xs:element ref="OperationalProtection" minOccurs="0"/>
3756           <xs:element ref="AuthnMethod"/>
3757           <xs:element ref="GoverningAgreements" minOccurs="0"/>
3758           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3759         </xs:sequence>
3760         <xs:attribute name="ID" type="xs:ID" use="optional"/>
3761       </xs:restriction>
3762     </xs:complexContent>
3763   </xs:complexType>
3764
3765   <xs:complexType name="AuthnMethodBaseType">
3766     <xs:complexContent>
3767       <xs:restriction base="AuthnMethodBaseType">
3768         <xs:sequence>
3769           <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
3770           <xs:element ref="Authenticator"/>
3771           <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
3772           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3773         </xs:sequence>
3774       </xs:restriction>
3775     </xs:complexContent>
3776   </xs:complexType>
3777
3778   <xs:complexType name="PrincipalAuthenticationMechanismType">
3779     <xs:complexContent>
3780       <xs:restriction base="PrincipalAuthenticationMechanismType">
3781         <xs:sequence>
3782           <xs:element ref="Token"/>
3783         </xs:sequence>
3784       </xs:restriction>
3785     </xs:complexContent>
3786   </xs:complexType>
3787
3788   <xs:complexType name="TokenType">
3789     <xs:complexContent>
3790       <xs:restriction base="TokenType">
3791         <xs:sequence>
3792           <xs:element ref="TimeSyncToken"/>
3793           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
3794         </xs:sequence>
3795       </xs:restriction>
3796     </xs:complexContent>
3797   </xs:complexType>
3798
3799   <xs:complexType name="TimeSyncTokenType">

```



```

3800     <xs:complexContent>
3801       <xs:restriction base="TimeSyncTokenType">
3802         <xs:attribute name="DeviceType" use="required">
3803           <xs:simpleType>
3804             <xs:restriction base="DeviceTypeType">
3805               <xs:enumeration value="hardware"/>
3806             </xs:restriction>
3807           </xs:simpleType>
3808         </xs:attribute>
3809
3810         <xs:attribute name="SeedLength" use="required">
3811           <xs:simpleType>
3812             <xs:restriction base="xs:integer">
3813               <xs:minInclusive value="64"/>
3814             </xs:restriction>
3815           </xs:simpleType>
3816         </xs:attribute>
3817
3818         <xs:attribute name="DeviceInHand" use="required">
3819           <xs:simpleType>
3820             <xs:restriction base="booleanType">
3821               <xs:enumeration value="true"/>
3822             </xs:restriction>
3823           </xs:simpleType>
3824         </xs:attribute>
3825       </xs:restriction>
3826     </xs:complexContent>
3827 </xs:complexType>
3828
3829 </xs:redefine>
3830
3831 </xs:schema>

```

3832 3.4.25 Unspecified

3833 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

3834 The Unspecified class indicates that the authentication was performed by unspecified means.

4 References

3835

- 3836 [RFC 1510] J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5)*. IETF
3837 RFC 1510, September 1993. See <http://www.ietf.org/rfc/rfc1510.txt>.
- 3838 [RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
3839 RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- 3840 [RFC 2945] T. Wu. *The SRP Authentication and Key Exchange System*. IETF RFC 2945,
3841 September 2000. See <http://www.ietf.org/rfc/rfc2945.txt>.
- 3842 [SAMLAC-xsd] J. Kemp et al. SAML authentication context schema. OASIS SSTC, March 2005.
3843 Document ID saml-schema-authn-context-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
3844 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 3845 [SAMLAC-Types] J. Kemp et al. SAML authentication context types schema. OASIS SSTC, March
3846 2005. Document ID saml-schema-authn-context-types-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
3847 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 3848 [SAMLAC-IP] J. Kemp et al. SAML context class schema for Internet Protocol. OASIS SSTC,
3849 March 2005. Document ID saml-schema-authn-context-ip-2.0. See
3850 <http://www.oasis-open.org/committees/security/>.
- 3851 [SAMLAC-IPP] J. Kemp et al. SAML context class schema for Internet Protocol Password.
3852 OASIS SSTC, March 2005. Document ID saml-schema-authn-context-ippword-
3853 2.0. See <http://www.oasis-open.org/committees/security/>.
- 3854 [SAMLAC-Kerb] J. Kemp et al. SAML context class schema for Kerberos. OASIS SSTC, March
3855 2005. Document ID saml-schema-authn-context-kerberos-2.0. See
3856 <http://www.oasis-open.org/committees/security/>.
- 3857 [SAMLAC-MOFC] J. Kemp et al. SAML context class schema for Mobile One Factor Contract.
3858 Document ID saml-schema-authn-context-mobileonefactor-reg-2.0. See OASIS
3859 SSTC, March 2005. <http://www.oasis-open.org/committees/security/>.
- 3860 [SAMLAC-MOFU] J. Kemp et al. SAML context class schema for Mobile One Factor Unregistered.
3861 Document ID saml-schema-authn-context-mobileonefactor-unreg-2.0. See
3862 OASIS SSTC, March 2005. <http://www.oasis-open.org/committees/security/>.
- 3863 [SAMLAC-MTFC] J. Kemp et al. SAML context class schema for Mobile Two Factor Contract.
3864 OASIS SSTC, March 2005. Document ID saml-schema-authn-context-
3865 mobiletwofactor-reg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 3866 [SAMLAC-MTFU] J. Kemp et al. SAML context class schema for Mobile Two Factor Unregistered.
3867 OASIS SSTC, March 2005. Document ID saml-schema-authn-context-
3868 mobiletwofactor-unreg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 3869 [SAMLAC-Pass] J. Kemp et al. SAML context class schema for Password. OASIS SSTC, March
3870 2005. Document ID saml-schema-authn-context-pword-2.0. See
3871 <http://www.oasis-open.org/committees/security/>.
- 3872 [SAMLAC-PGP] J. Kemp et al. SAML context class schema for Public Key – PGP. OASIS SSTC,
3873 March 2005. Document ID saml-schema-authn-context-pgp-2.0. See
3874 <http://www.oasis-open.org/committees/security/>.
- 3875 [SAMLAC-PPT] J. Kemp et al. SAML context class schema for Password Protected Transport.
3876 OASIS SSTC, March 2005. Document ID saml-schema-authn-context-ppt-2.0.
3877 See <http://www.oasis-open.org/committees/security/>.
- 3878 [SAMLAC-Prev] J. Kemp et al. SAML context class schema for Previous Session. OASIS SSTC,
3879 March 2005. Document ID saml-schema-authn-context-session-2.0. See
3880 <http://www.oasis-open.org/committees/security/>.
- 3881 [SAMLAC-Smart] J. Kemp et al. SAML context class schema for Smartcard. OASIS SSTC, March
3882 2005. Document ID saml-schema-authn-context-smartcard-2.0. See

3883		http://www.oasis-open.org/committees/security/ .
3884	[SAMLAC-SmPKI]	J. Kemp et al. SAML context class schema for Smartcard PKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-smartcardpki-2.0. See http://www.oasis-open.org/committees/security/ .
3885		
3886		
3887	[SAMLAC-SPKI]	J. Kemp et al. SAML context class schema for Public Key – SPKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-spki-2.0. See http://www.oasis-open.org/committees/security/ .
3888		
3889		
3890	[SAMLAC-SRP]	J. Kemp et al. SAML context class schema for Secure Remote Password. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-srp-2.0. See http://www.oasis-open.org/committees/security/ .
3891		
3892		
3893	[SAMLAC-SSL]	J. Kemp et al. SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-sslcrt-2.0. See http://www.oasis-open.org/committees/security/ .
3894		
3895		
3896	[SAMLAC-SwPKI]	J. Kemp et al. SAML context class schema for Software PKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-softwarepki-2.0. See http://www.oasis-open.org/committees/security/ .
3897		
3898		
3899	[SAMLAC-Tele]	J. Kemp et al. SAML context class schema for Telephony. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
3900		
3901		
3902	[SAMLAC-TNom]	J. Kemp et al. SAML context class schema for Telephony (“Nomadic”). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-nomad-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
3903		
3904		
3905	[SAMLAC-TPers]	J. Kemp et al. SAML context class schema for Telephony (Personalized). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-personal-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
3906		
3907		
3908	[SAMLAC-TAuthn]	J. Kemp et al. SAML context class schema for Telephony (Authenticated). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-auth-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
3909		
3910		
3911	[SAMLAC-TST]	J. Kemp et al. SAML context class schema for Time Sync Token. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-timesync-2.0. See http://www.oasis-open.org/committees/security/ .
3912		
3913		
3914	[SAMLAC-X509]	J. Kemp et al. SAML context class schema for Public Key – X.509. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-x509-2.0. See http://www.oasis-open.org/committees/security/ .
3915		
3916		
3917	[SAMLAC-XSig]	J. Kemp et al. SAML context class schema for Public Key – XML Signature. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-xmlsig-2.0. See http://www.oasis-open.org/committees/security/ .
3918		
3919		
3920	[SAMLCore]	S. Cantor et al. <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-core-2.0-os. See http://www.oasis-open.org/committees/security/ .
3921		
3922		
3923	[Schema1]	H. S. Thompson et al. <i>XML Schema Part 1: Structures</i> . World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/xmlschema-1/ .
3924		
3925		
3926	[XMLSig]	D. Eastlake et al., <i>XML-Signature Syntax and Processing</i> , World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/xmlsig-core/ .
3927		
3928		

3929 Appendix A. Acknowledgments

3930 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
3931 Committee, whose voting members at the time of publication were:

- 3932 • Conor Cahill, AOL
- 3933 • John Hughes, Atos Origin
- 3934 • Hal Lockhart, BEA Systems
- 3935 • Mike Beach, Boeing
- 3936 • Rebekah Metz, Booz Allen Hamilton
- 3937 • Rick Randall, Booz Allen Hamilton
- 3938 • Ronald Jacobson, Computer Associates
- 3939 • Gavenraj Sodhi, Computer Associates
- 3940 • Thomas Wisniewski, Entrust
- 3941 • Carolina Canales-Valenzuela, Ericsson
- 3942 • Dana Kaufman, Forum Systems
- 3943 • Irving Reid, Hewlett-Packard
- 3944 • Guy Denton, IBM
- 3945 • Heather Hinton, IBM
- 3946 • Maryann Hondo, IBM
- 3947 • Michael McIntosh, IBM
- 3948 • Anthony Nadalin, IBM
- 3949 • Nick Ragouzis, Individual
- 3950 • Scott Cantor, Internet2
- 3951 • Bob Morgan, Internet2
- 3952 • Peter Davis, Neustar
- 3953 • Jeff Hodges, Neustar
- 3954 • Frederick Hirsch, Nokia
- 3955 • Senthil Sengodan, Nokia
- 3956 • Abbie Barbir, Nortel Networks
- 3957 • Scott Kiestler, Novell
- 3958 • Cameron Morris, Novell
- 3959 • Paul Madsen, NTT
- 3960 • Steve Anderson, OpenNetwork
- 3961 • Ari Kermaier, Oracle
- 3962 • Vamsi Motukuru, Oracle
- 3963 • Darren Platt, Ping Identity
- 3964 • Prateek Mishra, Principal Identity
- 3965 • Jim Lien, RSA Security
- 3966 • John Linn, RSA Security
- 3967 • Rob Philpott, RSA Security
- 3968 • Dipak Chopra, SAP
- 3969 • Jahan Moreh, Sigaba
- 3970 • Bhavna Bhatnagar, Sun Microsystems
- 3971 • Eve Maler, Sun Microsystems

- 3972 • Ronald Monzillo, Sun Microsystems
- 3973 • Emily Xu, Sun Microsystems
- 3974 • Greg Whitehead, Trustgenix
- 3975

3976 The editors also would like to acknowledge the following former SSTC members for their contributions to
3977 this or previous versions of the OASIS Security Assertions Markup Language Standard:

- 3978 • Stephen Farrell, Baltimore Technologies
- 3979 • David Orchard, BEA Systems
- 3980 • Krishna Sankar, Cisco Systems
- 3981 • Zahid Ahmed, CommerceOne
- 3982 • Tim Alsop, CyberSafe Limited
- 3983 • Carlisle Adams, Entrust
- 3984 • Tim Moses, Entrust
- 3985 • Nigel Edwards, Hewlett-Packard
- 3986 • Joe Pato, Hewlett-Packard
- 3987 • Bob Blakley, IBM
- 3988 • Marlena Erdos, IBM
- 3989 • Marc Chanliau, Netegrity
- 3990 • Chris McLaren, Netegrity
- 3991 • Lynne Rosenthal, NIST
- 3992 • Mark Skall, NIST
- 3993 • Charles Knouse, Oblix
- 3994 • Simon Godik, Overxeer
- 3995 • Charles Norwood, SAIC
- 3996 • Evan Prodromou, Securant
- 3997 • Robert Griffin, RSA Security (former editor)
- 3998 • Sai Allarvarpu, Sun Microsystems
- 3999 • Gary Ellison, Sun Microsystems
- 4000 • Chris Ferris, Sun Microsystems
- 4001 • Mike Myers, Traceroute Security
- 4002 • Phillip Hallam-Baker, VeriSign (former editor)
- 4003 • James Vanderbeek, Vodafone
- 4004 • Mark O'Neill, Vordel
- 4005 • Tony Palmer, Vordel

4006
4007 Finally, the editors wish to acknowledge the following people for their contributions of material used as
4008 input to the OASIS Security Assertions Markup Language specifications:

- 4009 • Thomas Gross, IBM
- 4010 • Birgit Pfitzmann, IBM

4011 **Appendix B. Notices**

4012 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
4013 might be claimed to pertain to the implementation or use of the technology described in this document or
4014 the extent to which any license under such rights might or might not be available; neither does it represent
4015 that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to
4016 rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made
4017 available for publication and any assurances of licenses to be made available, or the result of an attempt
4018 made to obtain a general license or permission for the use of such proprietary rights by implementors or
4019 users of this specification, can be obtained from the OASIS Executive Director.

4020 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or
4021 other proprietary rights which may cover technology that may be required to implement this specification.
4022 Please address the information to the OASIS Executive Director.

4023 **Copyright © OASIS Open 2005. All Rights Reserved.**

4024 This document and translations of it may be copied and furnished to others, and derivative works that
4025 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and
4026 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
4027 this paragraph are included on all such copies and derivative works. However, this document itself does
4028 not be modified in any way, such as by removing the copyright notice or references to OASIS, except as
4029 needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights
4030 defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it
4031 into languages other than English.

4032 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
4033 or assigns.

4034 This document and the information contained herein is provided on an "AS IS" basis and OASIS
4035 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
4036 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR
4037 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.