



1

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

5 **Committee Draft 01, 18 August 2004**

6 **Document identifier:**

7 sstc-saml-authn-context-2.0-cd-01

8 **Location:**

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

10 **Editors:**

11 John Kemp, Nokia
12 Rob Philpott, RSA Security
13 Eve Maler, Sun Microsystems

14 **SAML V2.0 Contributors:**

15 Conor P. Cahill, AOL
16 Hal Lockhart, BEA Systems
17 Michael Beach, Boeing
18 Rick Randall, Boozé, Allen, Hamilton
19 Tim Alsop, Cybersafe
20 Nick Ragouzis, Enosis
21 John Hughes, Entegrity Solutions
22 Paul Madsen, Entrust
23 Irving Reid, Hewlett-Packard
24 Paula Austel, IBM
25 Maryann Hondo, IBM
26 Michael McIntosh, IBM
27 Tony Nadalin, IBM
28 Scott Cantor, Internet2
29 RL 'Bob' Morgan, Internet2
30 Rebekah Metz, NASA
31 Prateek Mishra, Netegrity
32 Peter C Davis, Neustar
33 Frederick Hirsch, Nokia
34 John Kemp, Nokia
35 Charles Knouse, Oblix
36 Steve Anderson, OpenNetwork
37 John Linn, RSA Security
38 Rob Philpott, RSA Security
39 Jahan Moreh, Sigaba
40 Anne Anderson, Sun Microsystems
41 Jeff Hodges, Sun Microsystems
42 Eve Maler, Sun Microsystems
43 Ron Monzillo, Sun Microsystems
44 Greg Whitehead, Trustgenix

45 **Abstract:**

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

48 **Status:**

49 This is a **Committee Draft** approved by the Security Services Technical Committee on 17 August
50 2004.

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

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

60 Table of Contents

61	1	Introduction.....	4
62	1.1	Authentication Context Concepts.....	4
63	1.2	Notation and Terminology.....	4
64	2	Authentication Context Declaration.....	6
65	2.1	Data Model.....	6
66	2.2	Extensibility.....	7
67	2.3	Processing Rules.....	7
68	2.4	Schema.....	7
69	3	Authentication Context Classes.....	24
70	3.1	Advantages of Authentication Context Classes.....	24
71	3.2	Processing Rules.....	24
72	3.3	Extensibility.....	25
73	3.4	Schemas.....	25
74	3.4.1	Internet Protocol.....	25
75	3.4.2	InternetProtocolPassword.....	27
76	3.4.3	Kerberos.....	28
77	3.4.4	MobileOneFactorUnregistered.....	30
78	3.4.5	MobileTwoFactorUnregistered.....	33
79	3.4.6	MobileOneFactorContract.....	37
80	3.4.7	MobileTwoFactorContract.....	40
81	3.4.8	Password.....	43
82	3.4.9	PasswordProtectedTransport.....	45
83	3.4.10	PreviousSession.....	46
84	3.4.11	Public Key – X.509.....	48
85	3.4.12	Public Key – PGP.....	49
86	3.4.13	Public Key – SPKI.....	51
87	3.4.14	Public Key - XML Digital Signature.....	53
88	3.4.15	Smartcard.....	55
89	3.4.16	SmartcardPKI.....	56
90	3.4.17	SoftwarePKI.....	58
91	3.4.18	Telephony.....	61
92	3.4.19	Telephony ("Nomadic").....	62
93	3.4.20	Telephony (Personalized).....	63
94	3.4.21	Telephony (Authenticated).....	65
95	3.4.22	Secure Remote Password.....	66
96	3.4.23	SSL/TLS Certificate-Based Client Authentication.....	68
97	3.4.24	TimeSyncToken.....	70
98	3.4.25	Unspecified.....	72
99	4	References.....	73

100

101 1 Introduction

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

104 1.1 Authentication Context Concepts

105 If a service provider is to rely on the authentication of a Principal by an authentication authority (or more
106 generally of another provider by an authentication authority), the service provider may require information
107 additional to the assertion itself in order to assess the level of confidence they can place in that assertion.
108 This specification defines an XML Schema for the creation of Authentication Context declarations - XML
109 documents that allow the authentication authority to provide to the service provider this additional
110 information. Additionally, this specification defines a number of Authentication Context classes; categories
111 into which many Authentication Context declarations will fall, thereby simplifying their interpretation.

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

117 The choices that an authentication authority makes here will be driven in large part by the requirements of
118 the service providers with which the authentication authority has affiliated. These requirements
119 themselves will be determined by the nature of the service (that is, the sensitivity of any information
120 exchanged, the associated financial value, the service providers' risk tolerance, etc.) that the service
121 provider will be providing to the Principal.

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

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

133 1.2 Notation and Terminology

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

137 `Listings of XML schemas appear like this.`

138

139 `Example code listings appear like this.`

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

145 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
146 their respective namespaces as follows, whether or not a namespace declaration is present in the
147 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]. In schema listings, this is the default namespace and no prefix is shown. For clarity, the prefix is generally shown in specification text when XML Schema-related constructs are mentioned.
xsi:	http://www.w3.org/2001/XMLSchema-instance	This namespace is defined in the W3C XML Schema specification [Schema1] for schema-related markup that appears in XML instances.

148

149 This specification uses the following typographical conventions in text: <SAML**E**lement>,
150 <ns:Foreign**E**lement>, XMLAttribute, **Datatype**, Other**K**eyword.

2 Authentication Context Declaration

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

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

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

165 A SAML authentication authority will deliver to a relying party the additional authentication context
166 information in the form of an authentication context declaration, an XML document either inserted directly
167 or referenced within the authentication response message that the authentication authority returns to the
168 relying party.

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

2.1 Data Model

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

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

193 2.2 Extensibility

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

199 2.3 Processing Rules

200 Additional processing rules for authentication context declarations are specified in the SAML assertions
201 and protocols specification [SAMLCore].

202 2.4 Schema

203 This section lists the complete Authentication Context XML Schema.

```
204 <?xml version="1.0" encoding="UTF-8"?>
205 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
206   xmlns:xs="http://www.w3.org/2001/XMLSchema"
207   xmlns="urn:oasis:names:tc:SAML:2.0:ac">
208
209   <xs:element name="AuthenticationContextDeclaration"
210     type="AuthnContextDeclarationBaseType">
211     <xs:annotation>
212       <xs:documentation>
213         A particular assertion on an identity
214         provider's part with respect to the authentication
215         context associated with an authentication assertion.
216       </xs:documentation>
217     </xs:annotation>
218   </xs:element>
219
220   <xs:element name="Identification" type="IdentificationType">
221     <xs:annotation>
222       <xs:documentation>
223         Refers to those characteristics that describe the
224         processes and mechanisms
225         the Authentication Authority uses to initially create
226         an association between a Principal
227         and the identity (or name) by which the Principal will
228         be known
229       </xs:documentation>
230     </xs:annotation>
231   </xs:element>
232
233   <xs:element name="PhysicalVerification">
234     <xs:annotation>
235       <xs:documentation>
236         This element indicates that identification has been
237         performed in a physical
238         face-to-face meeting with the principal and not in an
239         online manner.
240       </xs:documentation>
241     </xs:annotation>
242     <xs:complexType>
243       <xs:attribute name="credentialLevel">
244         <xs:simpleType>
245           <xs:restriction base="xs:NMTOKEN">
```

```

246         <xs:enumeration value="primary"/>
247         <xs:enumeration value="secondary"/>
248     </xs:restriction>
249 </xs:simpleType>
250 </xs:attribute>
251 </xs:complexType>
252 </xs:element>
253
254 <xs:element name="WrittenConsent">
255     <xs:complexType>
256         <xs:sequence>
257             <xs:element ref="Extension" minOccurs="0"
258                 maxOccurs="unbounded"/>
259         </xs:sequence>
260     </xs:complexType>
261 </xs:element>
262
263 <xs:element name="TechnicalProtection"
264     type="TechnicalProtectionBaseType">
265     <xs:annotation>
266         <xs:documentation>
267             Refers to those characteristics that describe how the
268             'secret' (the knowledge or possession
269             of which allows the Principal to authenticate to the
270             Authentication Authority) is kept secure
271         </xs:documentation>
272     </xs:annotation>
273 </xs:element>
274
275 <xs:element name="SecretKeyProtection"
276     type="SecretKeyProtectionType">
277     <xs:annotation>
278         <xs:documentation>
279             This element indicates the types and strengths of
280             facilities
281             of a UA used to protect a shared secret key from
282             unauthorized access and/or use.
283         </xs:documentation>
284     </xs:annotation>
285 </xs:element>
286
287 <xs:element name="PrivateKeyProtection"
288     type="PrivateKeyProtectionType">
289     <xs:annotation>
290         <xs:documentation>
291             This element indicates the types and strengths of
292             facilities
293             of a UA used to protect a private key from
294             unauthorized access and/or use.
295         </xs:documentation>
296     </xs:annotation>
297 </xs:element>
298
299 <xs:element name="KeyActivation" type="KeyActivationType">
300     <xs:annotation>
301         <xs:documentation>The actions that must be performed
302             before the private key can be used. </xs:documentation>
303     </xs:annotation>
304 </xs:element>
305
306 <xs:element name="KeySharing" type="KeySharingType">

```



```

307     <xs:annotation>
308         <xs:documentation>Whether or not the private key is shared
309             with the certificate authority.</xs:documentation>
310     </xs:annotation>
311 </xs:element>
312
313 <xs:element name="KeyStorage" type="KeyStorageType">
314     <xs:annotation>
315         <xs:documentation>
316             In which medium is the key stored.
317             memory - the key is stored in memory.
318             smartcard - the key is stored in a smartcard.
319             token - the key is stored in a hardware token.
320             MobileDevice - the key is stored in a mobile device.
321             MobileAuthCard - the key is stored in a mobile
322             authentication card.
323         </xs:documentation>
324     </xs:annotation>
325 </xs:element>
326
327 <xs:element name="SubscriberLineNumber">
328     <xs:complexType>
329         <xs:sequence>
330             <xs:element ref="Extension" minOccurs="0"
331                 maxOccurs="unbounded"/>
332         </xs:sequence>
333     </xs:complexType>
334 </xs:element>
335
336 <xs:element name="UserSuffix">
337     <xs:complexType>
338         <xs:sequence>
339             <xs:element ref="Extension" minOccurs="0"
340                 maxOccurs="unbounded"/>
341         </xs:sequence>
342     </xs:complexType>
343 </xs:element>
344
345 <xs:element name="Password" type="PasswordType">
346     <xs:annotation>
347         <xs:documentation>
348             This element indicates that a password (or passphrase)
349             has been used to
350             authenticate the Principal to a remote system.
351         </xs:documentation>
352     </xs:annotation>
353 </xs:element>
354
355 <xs:element name="ActivationPin" type="ActivationPinType">
356     <xs:annotation>
357         <xs:documentation>
358             This element indicates that a Pin (Personal
359             Identification Number) has been used to authenticate the
360             Principal to
361             some local system in order to activate a key.
362         </xs:documentation>
363     </xs:annotation>
364 </xs:element>
365
366 <xs:element name="Token" type="TokenType">
367     <xs:annotation>

```

```

368     <xs:documentation>
369         This element indicates that a hardware or software
370         token is used
371         as a method of identifying the Principal.
372     </xs:documentation>
373 </xs:annotation>
374 </xs:element>
375
376 <xs:element name="TimeSyncToken" type="TimeSyncTokenType">
377     <xs:annotation>
378         <xs:documentation>
379             This element indicates that a time synchronization
380             token is used to identify the Principal. hardware -
381             the time synchronization
382             token has been implemented in hardware. software - the
383             time synchronization
384             token has been implemented in software. SeedLength -
385             the length, in bits, of the
386             random seed used in the time synchronization token.
387         </xs:documentation>
388     </xs:annotation>
389 </xs:element>
390
391 <xs:element name="Smartcard">
392     <xs:annotation>
393         <xs:documentation>
394             This element indicates that a smartcard is used to
395             identity the Principal.
396         </xs:documentation>
397     </xs:annotation>
398     <xs:complexType>
399         <xs:sequence>
400             <xs:element ref="Extension" minOccurs="0"
401                 maxOccurs="unbounded"/>
402         </xs:sequence>
403     </xs:complexType>
404 </xs:element>
405
406 <xs:element name="Length" type="LengthType">
407     <xs:annotation>
408         <xs:documentation>
409             This element indicates the minimum and/or maximum
410             ASCII length of the password which is enforced (by the UA
411             or the
412             IdP). In other words, this is the minimum and/or maximum
413             number of
414             ASCII characters required to represent a valid password.
415             min - the minimum number of ASCII characters required
416             in a valid password, as enforced by the UA or the IdP.
417             max - the maximum number of ASCII characters required
418             in a valid password, as enforced by the UA or the IdP.
419         </xs:documentation>
420     </xs:annotation>
421 </xs:element>
422
423 <xs:element name="ActivationLimit" type="ActivationLimitType">
424     <xs:annotation>
425         <xs:documentation>
426             This element indicates the length of time for which an
427             PIN-based authentication is valid.
428         </xs:documentation>

```

```

429     </xs:annotation>
430 </xs:element>
431
432 <xs:element name="Generation">
433   <xs:annotation>
434     <xs:documentation>
435       Indicates whether the password was chosen by the
436       Principal or auto-supplied by the Authentication
437 Authority.
438       principalchosen - the Principal is allowed to choose
439       the value of the password. This is true even if
440       the initial password is chosen at random by the UA or
441       the IdP and the Principal is then free to change
442       the password.
443       automatic - the password is chosen by the UA or the
444       IdP to be cryptographically strong in some sense,
445       or to satisfy certain password rules, and that the
446       Principal is not free to change it or to choose a new
447 password.
448     </xs:documentation>
449   </xs:annotation>
450
451   <xs:complexType>
452     <xs:attribute name="mechanism" use="required">
453       <xs:simpleType>
454         <xs:restriction base="xs:NMTOKEN">
455           <xs:enumeration value="principalchosen"/>
456           <xs:enumeration value="automatic"/>
457         </xs:restriction>
458       </xs:simpleType>
459     </xs:attribute>
460   </xs:complexType>
461 </xs:element>
462
463 <xs:element name="AuthenticationMethod"
464   type="AuthnMethodBaseType">
465   <xs:annotation>
466     <xs:documentation>
467       Refers to those characteristics that define the
468       mechanisms by which the Principal authenticates to the
469 Authentication
470 Authority.
471     </xs:documentation>
472   </xs:annotation>
473 </xs:element>
474
475 <xs:element name="PrincipalAuthenticationMechanism"
476   type="PrincipalAuthenticationMechanismType">
477   <xs:annotation>
478     <xs:documentation>
479       The method that a Principal employs to perform
480       authentication to local system components.
481     </xs:documentation>
482   </xs:annotation>
483 </xs:element>
484
485 <xs:element name="Authenticator" type="AuthenticatorBaseType">
486   <xs:annotation>
487     <xs:documentation>
488       The method applied to validate a principal's
489       authentication across a network

```

```

490     </xs:documentation>
491     </xs:annotation>
492 </xs:element>
493
494 <xs:element name="PreviousSession">
495   <xs:annotation>
496     <xs:documentation>
497       Indicates that the Principal has been strongly
498       authenticated in a previous session during which the IdP
499 has set a
500       cookie in the UA. During the present session the
501 Principal has only
502       been authenticated by the UA returning the cookie to the
503 IdP.
504     </xs:documentation>
505   </xs:annotation>
506   <xs:complexType>
507     <xs:sequence>
508       <xs:element ref="Extension" minOccurs="0"
509         maxOccurs="unbounded"/>
510     </xs:sequence>
511   </xs:complexType>
512 </xs:element>
513
514 <xs:element name="ResumeSession">
515   <xs:annotation>
516     <xs:documentation>
517       Rather like PreviousSession but using stronger
518       security. A secret that was established in a previous
519 session with
520       the Authentication Authority has been cached by the local
521 system and
522       is now re-used (e.g. a Master Secret is used to derive
523 new session
524       keys in TLS, SSL, WTLS).
525     </xs:documentation>
526   </xs:annotation>
527   <xs:complexType>
528     <xs:sequence>
529       <xs:element ref="Extension" minOccurs="0"
530         maxOccurs="unbounded"/>
531     </xs:sequence>
532   </xs:complexType>
533 </xs:element>
534
535 <xs:element name="ZeroKnowledge">
536   <xs:annotation>
537     <xs:documentation>
538       This element indicates that the Principal has been
539       authenticated by a zero knowledge technique as specified
540 in ISO/IEC
541       9798-5.
542     </xs:documentation>
543   </xs:annotation>
544   <xs:complexType>
545     <xs:sequence>
546       <xs:element ref="Extension" minOccurs="0"
547         maxOccurs="unbounded"/>
548     </xs:sequence>
549   </xs:complexType>
550 </xs:element>

```

```

551
552     <xs:element name="SharedSecretChallengeResponse"
553 type="SharedSecretChallengeResponseType"/>
554
555     <xs:complexType name="SharedSecretChallengeResponseType">
556       <xs:annotation>
557         <xs:documentation>
558           This element indicates that the Principal has been
559           authenticated by a challenge-response protocol utilizing
560 shared secret
561           keys and symmetric cryptography.
562         </xs:documentation>
563       </xs:annotation>
564       <xs:sequence>
565         <xs:element ref="Extension" minOccurs="0"
566           maxOccurs="unbounded"/>
567       </xs:sequence>
568       <xs:attribute name="method" type="xs:anyURI" use="optional"/>
569     </xs:complexType>
570
571     <xs:element name="DigSig" type="PublicKeyType">
572       <xs:annotation>
573         <xs:documentation>
574           This element indicates that the Principal has been
575           authenticated by a mechanism which involves the Principal
576 computing a
577           digital signature over at least challenge data provided
578 by the IdP.
579         </xs:documentation>
580       </xs:annotation>
581     </xs:element>
582
583     <xs:element name="AsymmetricDecryption" type="PublicKeyType">
584       <xs:annotation>
585         <xs:documentation>
586           The local system has a private key but it is used
587           in decryption mode, rather than signature mode. For
588 example, the
589           Authentication Authority generates a secret and encrypts
590 it using the
591           local system's public key: the local system then proves
592 it has
593           decrypted the secret.
594         </xs:documentation>
595       </xs:annotation>
596     </xs:element>
597
598     <xs:element name="AsymmetricKeyAgreement" type="PublicKeyType">
599       <xs:annotation>
600         <xs:documentation>
601           The local system has a private key and uses it for
602 shared secret key agreement with the Authentication
603 Authority (e.g.
604           via Diffie Helman).
605         </xs:documentation>
606       </xs:annotation>
607     </xs:element>
608
609     <xs:complexType name="PublicKeyType">
610       <xs:sequence>
611         <xs:element ref="Extension" minOccurs="0"

```

```

612         maxOccurs="unbounded"/>
613     </xs:sequence>
614     <xs:attribute name="keyValidation" use="optional"/>
615 </xs:complexType>
616
617 <xs:element name="IPAddress">
618     <xs:annotation>
619         <xs:documentation>
620             This element indicates that the Principal has been
621             authenticated through connection from a particular IP
622 address.
623         </xs:documentation>
624     </xs:annotation>
625     <xs:complexType>
626         <xs:sequence>
627             <xs:element ref="Extension" minOccurs="0"
628                 maxOccurs="unbounded"/>
629         </xs:sequence>
630     </xs:complexType>
631 </xs:element>
632
633 <xs:element name="SharedSecretDynamicPlaintext"
634 type="SharedSecretDynamicPlaintextType"/>
635
636 <xs:annotation>
637     <xs:documentation>
638         The local system and Authentication Authority
639         share a secret key. The local system uses this to encrypt a
640         randomised string to pass to the Authentication Authority.
641     </xs:documentation>
642 </xs:annotation>
643
644 <xs:complexType name="SharedSecretDynamicPlaintextType">
645     <xs:sequence>
646         <xs:element ref="Extension" minOccurs="0"
647             maxOccurs="unbounded"/>
648     </xs:sequence>
649 </xs:complexType>
650
651 <xs:element name="AuthenticatorTransportProtocol"
652 type="AuthenticatorTransportProtocolType">
653     <xs:annotation>
654         <xs:documentation>
655             The protocol across which Authenticator information is
656             transferred to an Authentication Authority verifier.
657         </xs:documentation>
658     </xs:annotation>
659 </xs:element>
660
661 <xs:element name="HTTP">
662     <xs:annotation>
663         <xs:documentation>
664             This element indicates that the Authenticator has been
665             transmitted using bare HTTP utilizing no additional
666 security
667             protocols.
668         </xs:documentation>
669     </xs:annotation>
670     <xs:complexType>
671         <xs:sequence>
672             <xs:element ref="Extension" minOccurs="0"

```

```

673         maxOccurs="unbounded"/>
674     </xs:sequence>
675 </xs:complexType>
676 </xs:element>
677
678 <xs:element name="IPSec">
679     <xs:annotation>
680         <xs:documentation>
681             This element indicates that the Authenticator has been
682             transmitted using a transport mechanism protected by an
683 IPSEC session.
684         </xs:documentation>
685     </xs:annotation>
686     <xs:complexType>
687         <xs:sequence>
688             <xs:element ref="Extension" minOccurs="0"
689                 maxOccurs="unbounded"/>
690         </xs:sequence>
691     </xs:complexType>
692 </xs:element>
693 <xs:element name="WTLS">
694     <xs:annotation>
695         <xs:documentation>
696             This element indicates that the Authenticator has been
697             transmitted using a transport mechanism protected by a
698 WTLS session.
699         </xs:documentation>
700     </xs:annotation>
701     <xs:complexType>
702         <xs:sequence>
703             <xs:element ref="Extension" minOccurs="0"
704                 maxOccurs="unbounded"/>
705         </xs:sequence>
706     </xs:complexType>
707 </xs:element>
708 <xs:element name="MobileNetworkNoEncryption">
709     <xs:annotation>
710         <xs:documentation>
711             This element indicates that the Authenticator has been
712             transmitted solely across a mobile network using no
713 additional
714             security mechanism.
715         </xs:documentation>
716     </xs:annotation>
717     <xs:complexType>
718         <xs:sequence>
719             <xs:element ref="Extension" minOccurs="0"
720                 maxOccurs="unbounded"/>
721         </xs:sequence>
722     </xs:complexType>
723 </xs:element>
724 <xs:element name="MobileNetworkRadioEncryption">
725     <xs:complexType>
726         <xs:sequence>
727             <xs:element ref="Extension" minOccurs="0"
728                 maxOccurs="unbounded"/>
729         </xs:sequence>
730     </xs:complexType>
731 </xs:element>
732 <xs:element name="MobileNetworkEndToEndEncryption">
733     <xs:complexType>

```

```

734     <xs:sequence>
735         <xs:element ref="Extension" minOccurs="0"
736             maxOccurs="unbounded"/>
737     </xs:sequence>
738 </xs:complexType>
739 </xs:element>
740
741 <xs:element name="SSL">
742     <xs:annotation>
743         <xs:documentation>
744             This element indicates that the Authenticator has been
745             transmitted using a transport mechanism protected by an
746             SSL or TLS
747             session.
748         </xs:documentation>
749     </xs:annotation>
750     <xs:complexType>
751         <xs:sequence>
752             <xs:element ref="Extension" minOccurs="0"
753                 maxOccurs="unbounded"/>
754         </xs:sequence>
755     </xs:complexType>
756 </xs:element>
757
758 <xs:element name="PSTN">
759     <xs:complexType>
760         <xs:sequence>
761             <xs:element ref="Extension" minOccurs="0"
762                 maxOccurs="unbounded"/>
763         </xs:sequence>
764     </xs:complexType>
765 </xs:element>
766
767 <xs:element name="ISDN">
768     <xs:complexType>
769         <xs:sequence>
770             <xs:element ref="Extension" minOccurs="0"
771                 maxOccurs="unbounded"/>
772         </xs:sequence>
773     </xs:complexType>
774 </xs:element>
775
776 <xs:element name="ADSL">
777     <xs:complexType>
778         <xs:sequence>
779             <xs:element ref="Extension" minOccurs="0"
780                 maxOccurs="unbounded"/>
781         </xs:sequence>
782     </xs:complexType>
783 </xs:element>
784
785 <xs:element name="OperationalProtection"
786     type="OperationalProtectionType">
787     <xs:annotation>
788         <xs:documentation>
789             Refers to those characteristics that describe
790             procedural security controls employed by the
791             Authentication Authority.
792         </xs:documentation>
793     </xs:annotation>
794 </xs:element>

```



```

795 <xs:element name="SecurityAudit" type="SecurityAuditType"/>
796
797
798 <xs:element name="SwitchAudit">
799   <xs:complexType>
800     <xs:sequence>
801       <xs:element ref="Extension" minOccurs="0"
802         maxOccurs="unbounded"/>
803     </xs:sequence>
804   </xs:complexType>
805 </xs:element>
806
807 <xs:element name="DeactivationCallCenter">
808   <xs:complexType>
809     <xs:sequence>
810       <xs:element ref="Extension" minOccurs="0"
811         maxOccurs="unbounded"/>
812     </xs:sequence>
813   </xs:complexType>
814 </xs:element>
815
816 <xs:element name="GoverningAgreements"
817   type="GoverningAgreementsType">
818   <xs:annotation>
819     <xs:documentation>
820       Provides a mechanism for linking to external (likely
821       human readable) documents in which additional business
822 agreements,
823       (e.g. liability constraints, obligations, etc) can be
824 placed.
825     </xs:documentation>
826   </xs:annotation>
827 </xs:element>
828
829 <xs:element name="GoverningAgreementRef"
830   type="GoverningAgreementRefType"/>
831
832 <xs:complexType name="IdentificationType">
833   <xs:sequence>
834     <xs:element ref="PhysicalVerification" minOccurs="0"/>
835     <xs:element ref="WrittenConsent" minOccurs="0"/>
836     <xs:element ref="Extension" minOccurs="0"
837       maxOccurs="unbounded"/>
838   </xs:sequence>
839   <xs:attribute name="nym">
840     <xs:annotation>
841       <xs:documentation>
842         This attribute indicates whether or not the
843         Identification mechanisms allow the actions of the
844 Principal to be
845         linked to an actual end user.
846       </xs:documentation>
847     </xs:annotation>
848     <xs:simpleType>
849       <xs:restriction base="xs:NMTOKEN">
850         <xs:enumeration value="anonymity"/>
851         <xs:enumeration value="verinymity"/>
852         <xs:enumeration value="pseudonymity"/>
853       </xs:restriction>
854     </xs:simpleType>
855   </xs:attribute>

```

```

856 </xs:complexType>
857
858 <xs:complexType name="GoverningAgreementsType">
859   <xs:sequence>
860     <xs:element ref="GoverningAgreementRef"
861       maxOccurs="unbounded"/>
862   </xs:sequence>
863 </xs:complexType>
864
865 <xs:complexType name="GoverningAgreementRefType">
866   <xs:attribute name="governingAgreementRef" type="xs:anyURI"
867     use="required"/>
868 </xs:complexType>
869
870 <xs:complexType name="AuthenticatorTransportProtocolType">
871   <xs:choice>
872     <xs:element ref="HTTP"/>
873     <xs:element ref="SSL"/>
874     <xs:element ref="MobileNetworkNoEncryption"/>
875     <xs:element ref="MobileNetworkRadioEncryption"/>
876     <xs:element ref="MobileNetworkEndToEndEncryption"/>
877     <xs:element ref="WTLS"/>
878     <xs:element ref="IPSec"/>
879     <xs:element ref="PSTN"/>
880     <xs:element ref="ISDN"/>
881     <xs:element ref="ADSL"/>
882     <xs:element ref="Extension" maxOccurs="unbounded"/>
883   </xs:choice>
884 </xs:complexType>
885
886 <xs:complexType name="PrincipalAuthenticationMechanismType">
887   <xs:sequence>
888     <xs:choice>
889       <xs:element ref="Password"/>
890       <xs:element ref="Token"/>
891       <xs:element ref="Smartcard"/>
892       <xs:element ref="ActivationPin"/>
893       <xs:element ref="Extension" maxOccurs="unbounded"/>
894     </xs:choice>
895   </xs:sequence>
896   <xs:attribute name="preauth" type="xs:integer"
897     use="optional"/>
898 </xs:complexType>
899
900 <xs:complexType name="AuthnMethodBaseType">
901   <xs:sequence>
902     <xs:element ref="PrincipalAuthenticationMechanism"
903       minOccurs="0"/>
904     <xs:element ref="Authenticator" minOccurs="0"/>
905     <xs:element ref="AuthenticatorTransportProtocol"
906       minOccurs="0"/>
907     <xs:element ref="Extension" minOccurs="0"
908       maxOccurs="unbounded"/>
909   </xs:sequence>
910 </xs:complexType>
911
912 <xs:complexType name="AuthnContextDeclarationBaseType">
913   <xs:sequence>
914     <xs:element ref="Identification" minOccurs="0"/>
915     <xs:element ref="TechnicalProtection" minOccurs="0"/>
916     <xs:element ref="OperationalProtection" minOccurs="0"/>

```

```

917     <xs:element ref="AuthenticationMethod" minOccurs="0"/>
918     <xs:element ref="GoverningAgreements" minOccurs="0"/>
919     <xs:element ref="Extension" minOccurs="0"
920       maxOccurs="unbounded"/>
921   </xs:sequence>
922   <xs:attribute name="ID" type="xs:ID"/>
923 </xs:complexType>
924
925 <xs:complexType name="TechnicalProtectionBaseType">
926   <xs:choice>
927     <xs:element ref="PrivateKeyProtection" minOccurs="0"/>
928     <xs:element ref="SecretKeyProtection" minOccurs="0"/>
929     <xs:element ref="Extension" minOccurs="0"
930       maxOccurs="unbounded"/>
931   </xs:choice>
932 </xs:complexType>
933
934 <xs:complexType name="OperationalProtectionType">
935   <xs:sequence>
936     <xs:element ref="SecurityAudit" minOccurs="0"/>
937     <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
938     <xs:element ref="Extension" minOccurs="0"
939       maxOccurs="unbounded"/>
940   </xs:sequence>
941 </xs:complexType>
942
943 <xs:complexType name="AuthenticatorBaseType">
944   <xs:choice>
945     <xs:element ref="PreviousSession"/>
946     <xs:element ref="ResumeSession"/>
947     <xs:element ref="DigSig"/>
948     <xs:element ref="Password"/>
949     <xs:element ref="ZeroKnowledge"/>
950     <xs:element ref="SharedSecretChallengeResponse"/>
951     <xs:element ref="SharedSecretDynamicPlaintext"/>
952     <xs:element ref="IPAddress"/>
953     <xs:element ref="AsymmetricDecryption"/>
954     <xs:element ref="AsymmetricKeyAgreement"/>
955     <xs:element ref="SubscriberLineNumber"/>
956     <xs:element ref="UserSuffix"/>
957     <xs:element ref="Extension" maxOccurs="unbounded"/>
958   </xs:choice>
959 </xs:complexType>
960
961 <xs:complexType name="KeyActivationType">
962   <xs:choice>
963     <xs:element ref="ActivationPin"/>
964     <xs:element ref="Extension" maxOccurs="unbounded"/>
965   </xs:choice>
966 </xs:complexType>
967
968 <xs:complexType name="KeySharingType">
969   <xs:attribute name="sharing" type="xs:boolean"
970     use="required"/>
971 </xs:complexType>
972
973 <xs:complexType name="PrivateKeyProtectionType">
974   <xs:sequence>
975     <xs:element ref="KeyActivation" minOccurs="0"/>
976     <xs:element ref="KeyStorage" minOccurs="0"/>
977     <xs:element ref="KeySharing" minOccurs="0"/>

```

```

978     <xs:element ref="Extension" minOccurs="0"
979         maxOccurs="unbounded"/>
980     </xs:sequence>
981 </xs:complexType>
982
983 <xs:complexType name="PasswordType">
984     <xs:sequence>
985         <xs:element ref="Length" minOccurs="0"/>
986         <xs:element ref="Alphabet" minOccurs="0"/>
987         <xs:element ref="Generation" minOccurs="0"/>
988         <xs:element ref="Extension" minOccurs="0"
989             maxOccurs="unbounded"/>
990     </xs:sequence>
991     <xs:attribute name="ExternalVerification" type="xs:anyURI"
992 use="optional"/>
993 </xs:complexType>
994
995 <xs:element name="RestrictedPassword"
996 type="RestrictedPasswordType"/>
997
998 <xs:complexType name="RestrictedPasswordType">
999     <xs:complexContent>
1000         <xs:restriction base="PasswordType">
1001             <xs:sequence>
1002                 <xs:element ref="RestrictedLength" minOccurs="1"/>
1003                 <xs:element ref="Generation" minOccurs="0"/>
1004                 <xs:element ref="Extension" minOccurs="0"
1005 maxOccurs="unbounded"/>
1006             </xs:sequence>
1007             <xs:attribute name="ExternalVerification"
1008 type="xs:anyURI" use="optional"/>
1009         </xs:restriction>
1010     </xs:complexContent>
1011 </xs:complexType>
1012
1013 <xs:element name="RestrictedLength"
1014 type="RestrictedLengthType"/>
1015
1016 <xs:complexType name="RestrictedLengthType">
1017     <xs:complexContent>
1018         <xs:restriction base="LengthType">
1019             <xs:attribute name="min" use="required">
1020                 <xs:simpleType>
1021                     <xs:restriction base="xs:integer">
1022                         <xs:minInclusive value="3"/>
1023                     </xs:restriction>
1024                 </xs:simpleType>
1025             </xs:attribute>
1026             <xs:attribute name="max" type="xs:integer"
1027 use="optional"/>
1028         </xs:restriction>
1029     </xs:complexContent>
1030 </xs:complexType>
1031
1032 <xs:complexType name="ActivationPinType">
1033     <xs:sequence>
1034         <xs:element ref="Length" minOccurs="0"/>
1035         <xs:element ref="Alphabet" minOccurs="0"/>
1036         <xs:element ref="Generation" minOccurs="0"/>
1037         <xs:element ref="ActivationLimit" minOccurs="0"/>
1038         <xs:element ref="Extension" minOccurs="0"

```

```

1039         maxOccurs="unbounded"/>
1040     </xs:sequence>
1041 </xs:complexType>
1042 <xs:element name="Alphabet" type="AlphabetType"/>
1043 <xs:complexType name="AlphabetType">
1044     <xs:attribute name="requiredChars" type="xs:string"
1045         use="required"/>
1046     <xs:attribute name="excludedChars" type="xs:string"
1047         use="optional"/>
1048     <xs:attribute name="case" type="xs:string" use="optional"/>
1049 </xs:complexType>
1050 <xs:complexType name="TokenType">
1051     <xs:sequence>
1052         <xs:element ref="TimeSyncToken"/>
1053         <xs:element ref="Extension" minOccurs="0"
1054             maxOccurs="unbounded"/>
1055     </xs:sequence>
1056 </xs:complexType>
1057 <xs:complexType name="TimeSyncTokenType">
1058     <xs:attribute name="DeviceType" use="required">
1059         <xs:simpleType>
1060             <xs:restriction base="xs:NMTOKEN">
1061                 <xs:enumeration value="hardware"/>
1062                 <xs:enumeration value="software"/>
1063             </xs:restriction>
1064         </xs:simpleType>
1065     </xs:attribute>
1066     <xs:attribute name="SeedLength" type="xs:integer"
1067         use="required"/>
1068     <xs:attribute name="DeviceInHand" use="required">
1069         <xs:simpleType>
1070             <xs:restriction base="xs:NMTOKEN">
1071                 <xs:enumeration value="true"/>
1072                 <xs:enumeration value="false"/>
1073             </xs:restriction>
1074         </xs:simpleType>
1075     </xs:attribute>
1076 </xs:complexType>
1077 <xs:complexType name="ActivationLimitType">
1078     <xs:choice>
1079         <xs:element ref="ActivationLimitDuration"/>
1080         <xs:element ref="ActivationLimitUsages"/>
1081         <xs:element ref="ActivationLimitSession"/>
1082     </xs:choice>
1083 </xs:complexType>
1084 <xs:element name="ActivationLimitDuration"
1085     type="ActivationLimitDurationType">
1086     <xs:annotation>
1087         <xs:documentation>
1088             This element indicates that the Key Activation Limit is
1089             defined as a specific duration of time.
1090         </xs:documentation>
1091     </xs:annotation>
1092 </xs:element>
1093 <xs:element name="ActivationLimitUsages"
1094     type="ActivationLimitUsagesType">
1095     <xs:annotation>
1096         <xs:documentation>
1097             This element indicates that the Key Activation Limit is
1098             defined as a number of usages.
1099         </xs:documentation>

```

```

1100     </xs:annotation>
1101 </xs:element>
1102 <xs:element name="ActivationLimitSession"
1103     type="ActivationLimitSessionType">
1104     <xs:annotation>
1105         <xs:documentation>
1106             This element indicates that the Key Activation Limit is
1107             the session.
1108         </xs:documentation>
1109     </xs:annotation>
1110 </xs:element>
1111 <xs:complexType name="ActivationLimitDurationType">
1112     <xs:attribute name="duration" type="xs:duration"
1113         use="required"/>
1114 </xs:complexType>
1115 <xs:complexType name="ActivationLimitUsagesType">
1116     <xs:attribute name="number" type="xs:integer"
1117         use="required"/>
1118 </xs:complexType>
1119 <xs:complexType name="ActivationLimitSessionType"/>
1120 <xs:complexType name="LengthType">
1121     <xs:attribute name="min" type="xs:integer" use="required"/>
1122     <xs:attribute name="max" type="xs:integer" use="optional"/>
1123 </xs:complexType>
1124
1125 <xs:complexType name="KeyStorageType">
1126     <xs:attribute name="medium" use="required">
1127         <xs:simpleType>
1128             <xs:restriction base="xs:NMTOKEN">
1129                 <xs:enumeration value="memory"/>
1130                 <xs:enumeration value="smartcard"/>
1131                 <xs:enumeration value="token"/>
1132                 <xs:enumeration value="MobileDevice"/>
1133                 <xs:enumeration value="MobileAuthCard"/>
1134             </xs:restriction>
1135         </xs:simpleType>
1136     </xs:attribute>
1137 </xs:complexType>
1138
1139 <xs:complexType name="SecretKeyProtectionType">
1140     <xs:sequence>
1141         <xs:element ref="KeyActivation" minOccurs="0"/>
1142         <xs:element ref="KeyStorage" minOccurs="0"/>
1143         <xs:element ref="Extension" maxOccurs="unbounded"/>
1144     </xs:sequence>
1145 </xs:complexType>
1146
1147 <xs:complexType name="SecurityAuditType">
1148     <xs:sequence>
1149         <xs:element ref="SwitchAudit" minOccurs="0"/>
1150         <xs:element ref="Extension" minOccurs="0"
1151             maxOccurs="unbounded"/>
1152     </xs:sequence>
1153 </xs:complexType>
1154
1155 <xs:element name="Extension" type="ExtensionType"/>
1156
1157 <xs:complexType name="ExtensionType">
1158     <xs:sequence>
1159         <xs:any namespace="##other" processContents="lax"
1160             maxOccurs="unbounded"/>

```

1161
1162
1163
1164

```
</xs:sequence>  
</xs:complexType>  
</xs:schema>
```

1165 3 Authentication Context Classes

1166 The number of permutations of different characteristics ensures that there is a theoretically infinite number
1167 of unique authentication contexts. The implication is that, in theory, any particular relying party would be
1168 expected to be able to parse arbitrary authentication context declarations and, more importantly, to
1169 analyze the declaration in order to assess the “quality” of the associated authentication assertion. Making
1170 such an assessment is non-trivial.

1171 Fortunately, an optimization is possible. In practice many authentication contexts will fall into categories
1172 determined by industry practices and technology. For instance, many B2C web browser authentication
1173 contexts will be (partially) defined by the principal authenticating to the authentication authority through the
1174 presentation of a password over an SSL protected session. In the enterprise world, certificate-based
1175 authentication will be more common. Of course, the full authentication context is not limited to the
1176 specifics of how the principal authenticated. Nevertheless, the authentication method is often the most
1177 visible characteristic and as such, can serve as a useful classifier for a class of related authentication
1178 contexts.

1179 The concept is expressed in this specification as a definition of a series of authentication context classes.
1180 Each class defines a proper subset of the full set of authentication contexts. Classes have been chosen
1181 as representative of the current practices and technologies for authentication technologies, and provide
1182 identity and service providers a convenient shorthand when referring to authentication context issues.

1183 For instance, an authentication authority may include with the complete authentication context declaration
1184 it provides to a service provider an assertion that the authentication context also belongs to one of the
1185 authentication classes defined here. For some service providers, this assertion is sufficient detail for it to
1186 be able to assign an appropriate level of confidence to the associated authentication assertion. Other
1187 service providers might prefer to examine the complete authentication context declaration itself. Likewise,
1188 the ability to refer to an authentication context class rather than being required to list the complete details
1189 of a specific authentication content will simplify how the service provider expresses its desires and/or
1190 requirements to an authentication authority.

1191 3.1 Advantages of Authentication Context Classes

1192 The introduction of the additional layer of classes and the definition of an initial list of representative and
1193 flexible classes are expected to:

- 1194 • Make it easier for the authentication authority and service provider to come to an agreement on what
1195 are acceptable authentication contexts by giving them a framework for discussion.
- 1196 • Make it easier for service providers to indicate their preferences when requesting a step-up
1197 authentication assertion from an authentication authority.
- 1198 • Simplify for service providers the burden of processing authentication context declarations by giving
1199 them the option of being satisfied by the associated class.
- 1200 • Protect service providers from impact of new authentication technologies.
- 1201 • Make it easier for authentication authorities to publish their authentication capabilities, for example,
1202 through WSDL.

1203 3.2 Processing Rules

1204 Further processing rules for authentication context classes are described in the SAML assertions and
1205 protocols specification [SAMLCore].

1206 3.3 Extensibility

1207 As does the core authentication context declaration schema, the separate authentication context classes
1208 schemas allow the `<Extension>` element in certain locations of the tree structure. In general, where the
1209 `<Extension>` element occurred as a child of a `<Choice>` element, this option was removed in creating
1210 the appropriate class schema definition as an extension of the base type. When the `<Extension>`
1211 element occurred as an optional child of a `<Sequence>` element, the `<Extension>` element was
1212 allowed to remain in addition to any required elements.

1213 Consequently, authentication context declarations can include the `<Extension>` element (with additional
1214 elements in different namespaces) and still conform to authentication context class schemas (if they meet
1215 the other requirements of the schema of course)

1216 The authentication context class schemas extend (as restrictions) appropriate type definitions in the core
1217 authentication context declaration schema. As an extension point, the authentication context classes
1218 schemas themselves can be extended – their type definitions serving as base types in some other
1219 schema (potentially defined by some community wishing a more tightly defined authentication context
1220 class). To prevent logical inconsistencies, any such extensions can only further constrain the type
1221 definitions of the core authentication context declaration schema. To enforce this constraint, the
1222 authentication context class schemas are defined with the `finalDefault="extension"` attribute on
1223 the `<schema>` element to prevent this type of extension derivation.

1224 Additional authentication context classes MAY be developed by groups other than the Security Services
1225 Technical Committee. OASIS members may wish to document and submit them for consideration by the
1226 SSTC in a future version of the specification, and other groups may simply wish to inform the committee
1227 of their work. Please refer to the SSTC web site for further details.

1228 Guidelines for the specification of new context classes are as follows:

- 1229 • Specify a URI that uniquely identifies the context class.
- 1230 • Provide contact information for the author of the class.
- 1231 • Provide a textual description of the circumstances under which this class should be used.
- 1232 • Provide a valid XML schema [Schema1] document implementing the class

1233 Authors of new classes are encouraged to review those classes defined within this specification in order to
1234 guide their work.

1235 3.4 Schemas

1236 Authentication context classes are listed in the following subsections. The classes are listed in
1237 alphabetical order; no other ranking is implied by the order of classes. Classes are uniquely identified by
1238 URIs with the following initial stem:

```
1239 urn:oasis:names:tc:SAML:2.0:ac:classes
```

1240 The class schemas are defined as extension by restriction of parts of the the base authentication context
1241 schema. XML instances that validate against a given authentication context class schema are said to
1242 conform to that authentication context class.

1243 3.4.1 Internet Protocol

1244 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol

1245 Note that this URI is also used as the target namespace in the corresponding authentication context class
1246 schema document [SAMLAC-IP]).

1247 The Internet Protocol class is identified when a Principal is authenticated through the use of a provided IP
1248 address.

```

1249 <?xml version="1.0" encoding="UTF-8"?>
1250
1251 <xs:schema
1252 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1253 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1254 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1255 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1256 finalDefault="extension">
1257
1258   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1259   schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1260
1261   <xs:annotation>
1262     <xs:documentation>
1263       urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
1264     </xs:documentation>
1265   </xs:annotation>
1266
1267   <xs:complexType name="AuthnContextDeclaration">
1268     <xs:complexContent>
1269       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1270         <xs:sequence>
1271           <xs:element ref="ac:Identification" minOccurs="0"/>
1272           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
1273           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
1274           <xs:element ref="AuthnMethod"/>
1275           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1276           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1277             maxOccurs="unbounded"/>
1278           <xs:element ref="ac:Extension" minOccurs="0"
1279             maxOccurs="unbounded"/>
1280         </xs:sequence>
1281         <xs:attribute name="ID" type="xs:ID"/>
1282       </xs:restriction>
1283     </xs:complexContent>
1284   </xs:complexType>
1285
1286   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1287
1288   <xs:complexType name="AuthnMethodType">
1289     <xs:complexContent>
1290       <xs:restriction base="ac:AuthnMethodBaseType">
1291         <xs:sequence>
1292           <xs:element ref="ac:PrincipalAuthenticationMechanism"
1293             minOccurs="0"/>
1294           <xs:element ref="Authenticator"/>
1295           <xs:element ref="ac:AuthenticatorTransportProtocol"
1296             minOccurs="0"/>
1297           <xs:element ref="ac:Extension" minOccurs="0"
1298             maxOccurs="unbounded"/>
1299         </xs:sequence>
1300       </xs:restriction>
1301     </xs:complexContent>
1302   </xs:complexType>
1303
1304   <xs:element name="Authenticator" type="InternetProtocolType"/>
1305
1306   <xs:complexType name="InternetProtocolType">
1307     <xs:complexContent>
1308       <xs:restriction base="ac:AuthenticatorBaseType">
1309         <xs:choice>
1310           <xs:element ref="ac:IPAddress"/>
1311         </xs:choice>
1312       </xs:restriction>
1313     </xs:complexContent>
1314   </xs:complexType>
1315

```

1316

```
</xs:schema>
```

1317 3.4.2 InternetProtocolPassword

1318 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword

1319 Note that this URI is also used as the target namespace in the corresponding authentication context class
1320 schema document [SAMLAC-IPP]).

1321 The Internet Protocol Password class is identified when a Principal is authenticated through the use of a
1322 provided IP address, in addition to username/password.

```
1323 <?xml version="1.0" encoding="UTF-8"?>
1324
1325 <xs:schema
1326 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolP
1327 assword"
1328 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1329 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1330 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
1331 finalDefault="extension">
1332
1333   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1334 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1335
1336   <xs:annotation>
1337     <xs:documentation>
1338       urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
1339     </xs:documentation>
1340   </xs:annotation>
1341
1342   <xs:complexType name="AuthnContextDeclaration">
1343     <xs:complexContent>
1344       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1345         <xs:sequence>
1346           <xs:element ref="ac:Identification" minOccurs="0"/>
1347           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
1348           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
1349           <xs:element ref="AuthnMethod"/>
1350           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1351           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1352             maxOccurs="unbounded"/>
1353           <xs:element ref="ac:Extension" minOccurs="0"
1354             maxOccurs="unbounded"/>
1355         </xs:sequence>
1356         <xs:attribute name="ID" type="xs:ID"/>
1357       </xs:restriction>
1358     </xs:complexContent>
1359   </xs:complexType>
1360
1361   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1362
1363   <xs:complexType name="AuthnMethodType">
1364     <xs:complexContent>
1365       <xs:restriction base="ac:AuthnMethodBaseType">
1366         <xs:sequence>
1367           <xs:element ref="ac:PrincipalAuthenticationMechanism"
1368 minOccurs="0"/>
1369           <xs:element ref="Authenticator"/>
1370           <xs:element ref="ac:AuthenticatorTransportProtocol"
1371             minOccurs="0"/>
1372           <xs:element ref="ac:Extension" minOccurs="0"
1373             maxOccurs="unbounded"/>
1374         </xs:sequence>
1375       </xs:restriction>
1376     </xs:complexContent>
```

```

1377 </xs:complexType>
1378
1379 <xs:element name="Authenticator" type="InternetProtocolType"/>
1380
1381 <xs:complexType name="InternetProtocolType">
1382   <xs:complexContent>
1383     <xs:restriction base="ac:AuthenticatorBaseType">
1384       <xs:sequence>
1385         <xs:element ref="ac:IPAddress"/>
1386         <xs:element ref="ac:Password"/>
1387         <xs:element ref="ac:Extension" minOccurs="0"
1388           maxOccurs="unbounded"/>
1389       </xs:sequence>
1390     </xs:restriction>
1391   </xs:complexContent>
1392 </xs:complexType>
1393
1394 </xs:schema>

```

1395 3.4.3 Kerberos

1396 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

1397 Note that this URI is also used as the target namespace in the corresponding authentication context class
 1398 schema document [SAMLAC-Kerb]).

1399 This class is defined for use when the Principal has authenticated using a password to a local
 1400 authentication authority, in order to acquire a Kerberos ticket. That Kerberos ticket is then used for
 1401 subsequent network authentication.

1402 **Note:** It is possible for the authentication authority to indicate (via this context class) a pre-
 1403 authentication data type which was used by the Kerberos Key Distribution Center [RFC 1510]
 1404 when authenticating the Principal. The method used by the authentication authority to obtain this
 1405 information is outside of the scope of this specification, but it is strongly recommended that a
 1406 trusted method be deployed to pass the pre-authentication data type and any other Kerberos
 1407 related context details (e.g. ticket lifetime) to the authentication authority.

```

1408 <?xml version="1.0" encoding="UTF-8"?>
1409
1410 <xs:schema
1411 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1412 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1413 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1414 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1415 finalDefault="extension">
1416
1417   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1418     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1419
1420   <xs:annotation>
1421     <xs:documentation>
1422       urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
1423     </xs:documentation>
1424   </xs:annotation>
1425
1426   <xs:complexType name="AuthnContextDeclaration">
1427     <xs:complexContent>
1428       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1429         <xs:sequence>
1430           <xs:element ref="ac:Identification" minOccurs="0"/>
1431           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
1432           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
1433           <xs:element ref="AuthnMethod"/>
1434           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1435           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"

```

```

1436         maxOccurs="unbounded"/>
1437         <xs:element ref="ac:Extension" minOccurs="0"
1438         maxOccurs="unbounded"/>
1439     </xs:sequence>
1440     <xs:attribute name="ID" type="xs:ID"/>
1441 </xs:restriction>
1442 </xs:complexContent>
1443 </xs:complexType>
1444
1445 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1446
1447 <xs:complexType name="AuthnMethodType">
1448     <xs:complexContent>
1449         <xs:restriction base="ac:AuthnMethodBaseType">
1450             <xs:sequence>
1451                 <xs:element ref="AuthnMechanism"/>
1452                 <xs:element ref="Authenticator"/>
1453                 <xs:element ref="ac:AuthenticatorTransportProtocol"
1454                 minOccurs="0"/>
1455                 <xs:element ref="ac:Extension" minOccurs="0"
1456                 maxOccurs="unbounded"/>
1457             </xs:sequence>
1458         </xs:restriction>
1459     </xs:complexContent>
1460 </xs:complexType>
1461
1462 <xs:element name="AuthnMechanism" type="PasswordAuthnMechanismType"/>
1463
1464 <xs:complexType name="PasswordAuthnMechanismType">
1465     <xs:complexContent>
1466         <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
1467             <xs:sequence>
1468                 <xs:choice>
1469                     <xs:element ref="ac:RestrictedPassword"/>
1470                 </xs:choice>
1471             </xs:sequence>
1472             <xs:attribute name="preauth" type="xs:integer" use="optional"/>
1473         </xs:restriction>
1474     </xs:complexContent>
1475 </xs:complexType>
1476
1477 <xs:element name="Authenticator" type="SharedSecretType"/>
1478
1479 <xs:complexType name="SharedSecretType">
1480     <xs:complexContent>
1481         <xs:restriction base="ac:AuthenticatorBaseType">
1482             <xs:choice>
1483                 <xs:element ref="SharedSecretChallengeResponse"/>
1484             </xs:choice>
1485         </xs:restriction>
1486     </xs:complexContent>
1487 </xs:complexType>
1488
1489     <xs:element name="SharedSecretChallengeResponse"
1490     type="ChallengeResponseType"/>
1491
1492     <xs:complexType name="ChallengeResponseType">
1493         <xs:complexContent>
1494             <xs:restriction base="ac:SharedSecretChallengeResponseType">
1495                 <xs:attribute name="method"
1496                 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos"/>
1497             </xs:restriction>
1498         </xs:complexContent>
1499     </xs:complexType>
1500
1501 </xs:schema>

```

1502 An example of an XML instance conforming to this class schema is as follows:

```

1503 <?xml version="1.0" encoding="UTF-8"?>
1504   <AuthnContextDeclaration
1505     xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1506     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1507     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos">
1508
1509     <AuthnMethod>
1510       <PasswordAuthnMechanism preauth="0">
1511         <ac:Password/>
1512       <PasswordAuthnMechanism>
1513       <Authenticator>
1514         <SharedSecretChallengeResponse
1515 method="urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos"/>
1516       </Authenticator>
1517     </AuthnMethod>
1518
1519   </AuthnContextDeclaration>

```

1520 3.4.4 MobileOneFactorUnregistered

1521 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered

1522 Note that this URI is also used as the target namespace in the corresponding authentication context class
1523 schema document [SAMLAC-MOFU]).

1524 Reflects no mobile customer registration procedures and an authentication of the mobile device without
1525 requiring explicit end-user interaction. Again, this context authenticates only the device and never the
1526 user, it is useful when services other than the mobile operator want to add a secure device authentication
1527 to their authentication process.

```

1528 <?xml version="1.0" encoding="UTF-8"?>
1529
1530 <xs:schema
1531 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered"
1532 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1533 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1534 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered"
1535 finalDefault="extension">
1536
1537   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1538 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1539
1540   <xs:annotation>
1541     <xs:documentation>
1542       urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
1543     </xs:documentation>
1544   </xs:annotation>
1545
1546   <xs:complexType name="AuthnContextDeclaration">
1547     <xs:complexContent>
1548       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1549         <xs:sequence>
1550           <xs:element ref="Identification" minOccurs="0"/>
1551           <xs:element ref="TechnicalProtection" minOccurs="0"/>
1552           <xs:element ref="OperationalProtection" minOccurs="0"/>
1553           <xs:element ref="AuthnMethod"/>
1554           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1555           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1556             maxOccurs="unbounded"/>
1557           <xs:element ref="ac:Extension" minOccurs="0"
1558             maxOccurs="unbounded"/>
1559         </xs:sequence>
1560         <xs:attribute name="ID" type="xs:ID"/>
1561       </xs:restriction>
1562     </xs:complexContent>
1563   </xs:complexType>

```

```

1564     </xs:complexContent>
1565 </xs:complexType>
1566
1567 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1568
1569 <xs:complexType name="AuthnMethodType">
1570   <xs:complexContent>
1571     <xs:restriction base="ac:AuthnMethodBaseType">
1572       <xs:sequence>
1573         <xs:element ref="ac:PrincipalAuthenticationMechanism"
1574 minOccurs="0"/>
1575         <xs:element ref="Authenticator"/>
1576         <xs:element ref="AuthenticatorTransportProtocol"
1577 minOccurs="0"/>
1578         <xs:element ref="ac:Extension" minOccurs="0"
1579 maxOccurs="unbounded"/>
1580       </xs:sequence>
1581     </xs:restriction>
1582   </xs:complexContent>
1583 </xs:complexType>
1584
1585 <xs:element name="Authenticator" type="AuthenticatorType"/>
1586
1587 <xs:complexType name="AuthenticatorType">
1588   <xs:complexContent>
1589     <xs:restriction base="ac:AuthenticatorBaseType">
1590       <xs:choice>
1591         <xs:element ref="ac:DigSig"/>
1592         <xs:element ref="ac:ZeroKnowledge"/>
1593         <xs:element ref="ac:SharedSecretChallengeResponse"/>
1594         <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
1595         <xs:element ref="ac:AsymmetricDecryption"/>
1596         <xs:element ref="ac:AsymmetricKeyAgreement"/>
1597       </xs:choice>
1598     </xs:restriction>
1599   </xs:complexContent>
1600 </xs:complexType>
1601
1602 <xs:element name="AuthenticatorTransportProtocol"
1603 type="SecureTransportType"/>
1604
1605 <xs:complexType name="SecureTransportType">
1606   <xs:complexContent>
1607     <xs:restriction base="ac:AuthenticatorTransportProtocolType">
1608       <xs:choice>
1609         <xs:element ref="ac:SSL"/>
1610         <xs:element ref="ac:MobileNetworkRadioEncryption"/>
1611         <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
1612         <xs:element ref="ac:WTLS"/>
1613       </xs:choice>
1614     </xs:restriction>
1615   </xs:complexContent>
1616 </xs:complexType>
1617
1618 <xs:element name="OperationalProtection"
1619 type="OperationalProtectionType"/>
1620
1621 <xs:complexType name="OperationalProtectionType">
1622   <xs:complexContent>
1623     <xs:restriction base="OperationalProtectionType">
1624       <xs:sequence>
1625         <xs:element ref="ac:SecurityAudit"/>
1626         <xs:element ref="ac:DeactivationCallCenter"/>
1627         <xs:element ref="ac:Extension" minOccurs="0"
1628 maxOccurs="unbounded"/>
1629       </xs:sequence>
1630     </xs:restriction>

```

```

1631     </xs:complexContent>
1632 </xs:complexType>
1633
1634 <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
1635
1636 <xs:complexType name="TechnicalProtectionType">
1637   <xs:complexContent>
1638     <xs:restriction base="ac:TechnicalProtectionBaseType">
1639       <xs:choice>
1640         <xs:element ref="PrivateKeyProtection"/>
1641         <xs:element ref="SecretKeyProtection"/>
1642       </xs:choice>
1643     </xs:restriction>
1644   </xs:complexContent>
1645 </xs:complexType>
1646
1647 <xs:element name="PrivateKeyProtection"
1648 type="PrivateKeyProtectionType"/>
1649
1650 <xs:complexType name="PrivateKeyProtectionType">
1651   <xs:complexContent>
1652     <xs:restriction base="ac:PrivateKeyProtectionType">
1653       <xs:sequence>
1654         <xs:element ref="KeyStorage"/>
1655         <xs:element ref="ac:Extension" minOccurs="0"
1656 maxOccurs="unbounded"/>
1657       </xs:sequence>
1658     </xs:restriction>
1659   </xs:complexContent>
1660 </xs:complexType>
1661
1662 <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>
1663
1664 <xs:complexType name="SecretKeyProtectionType">
1665   <xs:complexContent>
1666     <xs:restriction base="ac:SecretKeyProtectionType">
1667       <xs:sequence>
1668         <xs:element ref="KeyStorage"/>
1669         <xs:element ref="ac:Extension" minOccurs="0"
1670 maxOccurs="unbounded"/>
1671       </xs:sequence>
1672     </xs:restriction>
1673   </xs:complexContent>
1674 </xs:complexType>
1675
1676 <xs:element name="KeyStorage" type="KeyStorageType"/>
1677
1678 <xs:complexType name="KeyStorageType">
1679   <xs:complexContent>
1680     <xs:restriction base="ac:KeyStorageType">
1681       <xs:attribute name="medium" use="required">
1682         <xs:simpleType>
1683           <xs:restriction base="xs:NMTOKEN">
1684             <xs:enumeration value="MobileDevice"/>
1685             <xs:enumeration value="MobileAuthCard"/>
1686             <xs:enumeration value="smartcard"/>
1687           </xs:restriction>
1688         </xs:simpleType>
1689       </xs:attribute>
1690     </xs:restriction>
1691   </xs:complexContent>
1692 </xs:complexType>
1693
1694 <xs:element name="SecurityAudit" type="SecurityAuditType"/>
1695
1696 <xs:complexType name="SecurityAuditType">
1697   <xs:complexContent>

```



```

1698     <xs:restriction base="ac:SecurityAuditType">
1699         <xs:sequence>
1700             <xs:element ref="ac:SwitchAudit"/>
1701             <xs:element ref="ac:Extension" minOccurs="0"
1702 maxOccurs="unbounded"/>
1703         </xs:sequence>
1704     </xs:restriction>
1705 </xs:complexContent>
1706 </xs:complexType>
1707
1708 <xs:element name="Identification" type="IdentificationType"/>
1709
1710 <xs:complexType name="IdentificationType">
1711     <xs:complexContent>
1712         <xs:restriction base="ac:IdentificationType">
1713             <xs:attribute name="nym">
1714                 <xs:simpleType>
1715                     <xs:restriction base="xs:NMTOKEN">
1716                         <xs:enumeration value="anonymity"/>
1717                         <xs:enumeration value="pseudonymity"/>
1718                     </xs:restriction>
1719                 </xs:simpleType>
1720             </xs:attribute>
1721         </xs:restriction>
1722     </xs:complexContent>
1723 </xs:complexType>
1724
1725 </xs:schema>

```

1726 3.4.5 MobileTwoFactorUnregistered

1727 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered

1728 Note that this URI is also used as the target namespace in the corresponding authentication context class
1729 schema document [SAMLAC-MTFU]).

1730 Reflects no mobile customer registration procedures and a two-factor based authentication, such as
1731 secure device and user PIN. This context class is useful when a service other than the mobile operator
1732 wants to link their customer ID to a mobile supplied two-factor authentication service by capturing mobile
1733 phone data at enrollment.

```

1734 <?xml version="1.0" encoding="UTF-8"?>
1735
1736 <xs:schema
1737 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUn
1738 registered"
1739 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1740 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1741 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregister
1742 ed"
1743 finalDefault="extension">
1744
1745     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1746 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1747
1748     <xs:annotation>
1749         <xs:documentation>
1750             urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
1751         </xs:documentation>
1752     </xs:annotation>
1753
1754     <xs:complexType name="AuthnContextDeclaration">
1755         <xs:complexContent>
1756             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1757                 <xs:sequence>
1758                     <xs:element ref="Identification" minOccurs="0"/>

```

```

1759     <xs:element ref="TechnicalProtection" minOccurs="0"/>
1760     <xs:element ref="OperationalProtection" minOccurs="0"/>
1761     <xs:element ref="AuthnMethod"/>
1762     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1763     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1764         maxOccurs="unbounded"/>
1765     <xs:element ref="ac:Extension" minOccurs="0"
1766         maxOccurs="unbounded"/>
1767     </xs:sequence>
1768     <xs:attribute name="ID" type="xs:ID"/>
1769 </xs:restriction>
1770 </xs:complexContent>
1771 </xs:complexType>
1772
1773 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1774
1775 <xs:complexType name="AuthnMethodType">
1776     <xs:complexContent>
1777         <xs:restriction base="ac:AuthnMethodBaseType">
1778             <xs:sequence>
1779                 <xs:element ref="ac:PrincipalAuthenticationMechanism"
1780 minOccurs="0"/>
1781                 <xs:element ref="Authenticator"/>
1782                 <xs:element ref="AuthenticatorTransportProtocol"
1783                     minOccurs="0"/>
1784                 <xs:element ref="ac:Extension" minOccurs="0"
1785                     maxOccurs="unbounded"/>
1786             </xs:sequence>
1787         </xs:restriction>
1788     </xs:complexContent>
1789 </xs:complexType>
1790
1791 <xs:element name="Authenticator" type="AuthenticatorType"/>
1792
1793 <xs:complexType name="AuthenticatorType">
1794     <xs:complexContent>
1795         <xs:restriction base="ac:AuthenticatorBaseType">
1796             <xs:choice>
1797                 <xs:element ref="ac:DigSig"/>
1798                 <xs:element ref="ac:ZeroKnowledge"/>
1799                 <xs:element ref="ac:SharedSecretChallengeResponse"/>
1800                 <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
1801                 <xs:element ref="ac:AsymmetricDecryption"/>
1802                 <xs:element ref="ac:AsymmetricKeyAgreement"/>
1803             <xs:sequence>
1804                 <xs:element ref="ac:Password" minOccurs="1"/>
1805             <xs:choice>
1806                 <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
1807                 <xs:element ref="ac:SharedSecretChallengeResponse"/>
1808             </xs:choice>
1809                 <xs:element ref="ac:Extension" maxOccurs="unbounded"/>
1810             </xs:sequence>
1811         </xs:choice>
1812     </xs:restriction>
1813 </xs:complexContent>
1814 </xs:complexType>
1815
1816 <xs:element name="AuthenticatorTransportProtocol"
1817 type="SecureTransportType"/>
1818
1819 <xs:complexType name="SecureTransportType">
1820     <xs:complexContent>
1821         <xs:restriction base="ac:AuthenticatorTransportProtocolType">
1822             <xs:choice>
1823                 <xs:element ref="ac:SSL"/>
1824                 <xs:element ref="ac:MobileNetworkNoEncryption"/>
1825                 <xs:element ref="ac:MobileNetworkRadioEncryption"/>

```

```

1826         <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
1827         <xs:element ref="ac:WTLS"/>
1828     </xs:choice>
1829 </xs:restriction>
1830 </xs:complexContent>
1831 </xs:complexType>
1832
1833 <xs:element name="OperationalProtection"
1834 type="OperationalProtectionType"/>
1835
1836 <xs:complexType name="OperationalProtectionType">
1837     <xs:complexContent>
1838         <xs:restriction base="OperationalProtectionType">
1839             <xs:sequence>
1840                 <xs:element ref="ac:SecurityAudit"/>
1841                 <xs:element ref="ac:DeactivationCallCenter"/>
1842                 <xs:element ref="ac:Extension" minOccurs="0"
1843 maxOccurs="unbounded"/>
1844             </xs:sequence>
1845         </xs:restriction>
1846     </xs:complexContent>
1847 </xs:complexType>
1848
1849 <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
1850
1851 <xs:complexType name="TechnicalProtectionType">
1852     <xs:complexContent>
1853         <xs:restriction base="ac:TechnicalProtectionBaseType">
1854             <xs:choice>
1855                 <xs:element ref="PrivateKeyProtection"/>
1856                 <xs:element ref="SecretKeyProtection"/>
1857             </xs:choice>
1858         </xs:restriction>
1859     </xs:complexContent>
1860 </xs:complexType>
1861
1862 <xs:element name="PrivateKeyProtection"
1863 type="PrivateKeyProtectionType"/>
1864
1865 <xs:complexType name="PrivateKeyProtectionType">
1866     <xs:complexContent>
1867         <xs:restriction base="ac:PrivateKeyProtectionType">
1868             <xs:sequence>
1869                 <xs:element ref="KeyActivation"/>
1870                 <xs:element ref="KeyStorage"/>
1871                 <xs:element ref="ac:Extension" minOccurs="0"
1872 maxOccurs="unbounded"/>
1873             </xs:sequence>
1874         </xs:restriction>
1875     </xs:complexContent>
1876 </xs:complexType>
1877
1878 <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>
1879
1880 <xs:complexType name="SecretKeyProtectionType">
1881     <xs:complexContent>
1882         <xs:restriction base="ac:SecretKeyProtectionType">
1883             <xs:sequence>
1884                 <xs:element ref="KeyActivation"/>
1885                 <xs:element ref="KeyStorage"/>
1886                 <xs:element ref="ac:Extension" minOccurs="0"
1887 maxOccurs="unbounded"/>
1888             </xs:sequence>
1889         </xs:restriction>
1890     </xs:complexContent>
1891 </xs:complexType>
1892

```

```

1893 <xs:element name="KeyActivation" type="KeyActivationType"/>
1894
1895 <xs:complexType name="KeyActivationType">
1896 <xs:complexContent>
1897 <xs:restriction base="ac:KeyActivationType">
1898 <xs:sequence>
1899 <xs:element ref="ac:ActivationPin"/>
1900 <xs:element ref="ac:Extension" minOccurs="0"
maxOccurs="unbounded"/>
1901 </xs:sequence>
1902 </xs:restriction>
1903 </xs:complexContent>
1904 </xs:complexType>
1905
1906
1907 <xs:element name="KeyStorage" type="KeyStorageType"/>
1908
1909 <xs:complexType name="KeyStorageType">
1910 <xs:complexContent>
1911 <xs:restriction base="ac:KeyStorageType">
1912 <xs:attribute name="medium" use="required">
1913 <xs:simpleType>
1914 <xs:restriction base="xs:NMTOKEN">
1915 <xs:enumeration value="MobileDevice"/>
1916 <xs:enumeration value="MobileAuthCard"/>
1917 <xs:enumeration value="smartcard"/>
1918 </xs:restriction>
1919 </xs:simpleType>
1920 </xs:attribute>
1921 </xs:restriction>
1922 </xs:complexContent>
1923 </xs:complexType>
1924
1925 <xs:element name="SecurityAudit" type="SecurityAuditType"/>
1926
1927 <xs:complexType name="SecurityAuditType">
1928 <xs:complexContent>
1929 <xs:restriction base="ac:SecurityAuditType">
1930 <xs:sequence>
1931 <xs:element ref="ac:SwitchAudit"/>
1932 <xs:element ref="ac:Extension" minOccurs="0"
maxOccurs="unbounded"/>
1933 </xs:sequence>
1934 </xs:restriction>
1935 </xs:complexContent>
1936 </xs:complexType>
1937
1938
1939 <xs:element name="Identification" type="IdentificationType"/>
1940
1941 <xs:complexType name="IdentificationType">
1942 <xs:complexContent>
1943 <xs:restriction base="ac:IdentificationType">
1944 <xs:attribute name="nym">
1945 <xs:simpleType>
1946 <xs:restriction base="xs:NMTOKEN">
1947 <xs:enumeration value="anonymity"/>
1948 <xs:enumeration value="pseudonymity"/>
1949 </xs:restriction>
1950 </xs:simpleType>
1951 </xs:attribute>
1952 </xs:restriction>
1953 </xs:complexContent>
1954 </xs:complexType>
1955
1956 </xs:schema>

```

1957 3.4.6 MobileOneFactorContract

1958 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract

1959 Note that this URI is also used as the target namespace in the corresponding authentication context class
1960 schema document [SAMLAC-MOFC]).

1961 Reflects mobile contract customer registration procedures and a single factor authentication. For example,
1962 a digital signing device with tamper resistant memory for key storage, such as the mobile MSISDN, but no
1963 required PIN or biometric for real-time user authentication.

```
1964 <?xml version="1.0" encoding="UTF-8"?>
1965
1966 <xs:schema
1967 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorCo
1968 ntract"
1969 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1970 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1971 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
1972 finalDefault="extension">
1973
1974 <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1975 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1976
1977 <xs:annotation>
1978 <xs:documentation>
1979 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
1980 </xs:documentation>
1981 </xs:annotation>
1982
1983 <xs:complexType name="AuthnContextDeclaration">
1984 <xs:complexContent>
1985 <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1986 <xs:sequence>
1987 <xs:element ref="Identification" minOccurs="0"/>
1988 <xs:element ref="TechnicalProtection" minOccurs="0"/>
1989 <xs:element ref="OperationalProtection" minOccurs="0"/>
1990 <xs:element ref="AuthnMethod"/>
1991 <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1992 <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1993 maxOccurs="unbounded"/>
1994 <xs:element ref="ac:Extension" minOccurs="0"
1995 maxOccurs="unbounded"/>
1996 </xs:sequence>
1997 <xs:attribute name="ID" type="xs:ID"/>
1998 </xs:restriction>
1999 </xs:complexContent>
2000 </xs:complexType>
2001
2002 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2003
2004 <xs:complexType name="AuthnMethodType">
2005 <xs:complexContent>
2006 <xs:restriction base="ac:AuthnMethodBaseType">
2007 <xs:sequence>
2008 <xs:element ref="ac:PrincipalAuthenticationMechanism"
2009 minOccurs="0"/>
2010 <xs:element ref="Authenticator"/>
2011 <xs:element ref="AuthenticatorTransportProtocol"
2012 minOccurs="0"/>
2013 <xs:element ref="ac:Extension" minOccurs="0"
2014 maxOccurs="unbounded"/>
2015 </xs:sequence>
2016 </xs:restriction>
2017 </xs:complexContent>
2018 </xs:complexType>
```

2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085

```
<xs:element name="Authenticator" type="AuthenticatorType"/>
<xs:complexType name="AuthenticatorType">
  <xs:complexContent>
    <xs:restriction base="ac:AuthenticatorBaseType">
      <xs:choice>
        <xs:element ref="ac:DigSig"/>
        <xs:element ref="ac:ZeroKnowledge"/>
        <xs:element ref="ac:SharedSecretChallengeResponse"/>
        <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
        <xs:element ref="ac:AsymmetricDecryption"/>
        <xs:element ref="ac:AsymmetricKeyAgreement"/>
      </xs:choice>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:element name="AuthenticatorTransportProtocol"
type="SecureTransportType"/>

<xs:complexType name="SecureTransportType">
  <xs:complexContent>
    <xs:restriction base="ac:AuthenticatorTransportProtocolType">
      <xs:choice>
        <xs:element ref="ac:SSL"/>
        <xs:element ref="ac:MobileNetworkNoEncryption"/>
        <xs:element ref="ac:MobileNetworkRadioEncryption"/>
        <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
        <xs:element ref="ac:WTLS"/>
      </xs:choice>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:element name="OperationalProtection"
type="OperationalProtectionType"/>

<xs:complexType name="OperationalProtectionType">
  <xs:complexContent>
    <xs:restriction base="OperationalProtectionType">
      <xs:sequence>
        <xs:element ref="ac:SecurityAudit"/>
        <xs:element ref="ac:DeactivationCallCenter"/>
        <xs:element ref="ac:Extension" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>

<xs:complexType name="TechnicalProtectionType">
  <xs:complexContent>
    <xs:restriction base="ac:TechnicalProtectionBaseType">
      <xs:choice>
        <xs:element ref="PrivateKeyProtection"/>
        <xs:element ref="SecretKeyProtection"/>
      </xs:choice>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:element name="PrivateKeyProtection"
type="PrivateKeyProtectionType"/>
```

```

2086     <xs:complexType name="PrivateKeyProtectionType">
2087       <xs:complexContent>
2088         <xs:restriction base="ac:PrivateKeyProtectionType">
2089           <xs:sequence>
2090             <xs:element ref="KeyStorage"/>
2091             <xs:element ref="ac:Extension" minOccurs="0"
2092 maxOccurs="unbounded"/>
2093           </xs:sequence>
2094         </xs:restriction>
2095       </xs:complexContent>
2096     </xs:complexType>
2097
2098     <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>
2099
2100     <xs:complexType name="SecretKeyProtectionType">
2101       <xs:complexContent>
2102         <xs:restriction base="ac:SecretKeyProtectionType">
2103           <xs:sequence>
2104             <xs:element ref="KeyStorage"/>
2105             <xs:element ref="ac:Extension" minOccurs="0"
2106 maxOccurs="unbounded"/>
2107           </xs:sequence>
2108         </xs:restriction>
2109       </xs:complexContent>
2110     </xs:complexType>
2111
2112     <xs:element name="KeyStorage" type="KeyStorageType"/>
2113
2114     <xs:complexType name="KeyStorageType">
2115       <xs:complexContent>
2116         <xs:restriction base="ac:KeyStorageType">
2117           <xs:attribute name="medium" use="required">
2118             <xs:simpleType>
2119               <xs:restriction base="xs:NMTOKEN">
2120                 <xs:enumeration value="MobileDevice"/>
2121                 <xs:enumeration value="MobileAuthCard"/>
2122                 <xs:enumeration value="smartcard"/>
2123               </xs:restriction>
2124             </xs:simpleType>
2125           </xs:attribute>
2126         </xs:restriction>
2127       </xs:complexContent>
2128     </xs:complexType>
2129
2130     <xs:element name="SecurityAudit" type="SecurityAuditType"/>
2131
2132     <xs:complexType name="SecurityAuditType">
2133       <xs:complexContent>
2134         <xs:restriction base="ac:SecurityAuditType">
2135           <xs:sequence>
2136             <xs:element ref="ac:SwitchAudit"/>
2137             <xs:element ref="ac:Extension" minOccurs="0"
2138 maxOccurs="unbounded"/>
2139           </xs:sequence>
2140         </xs:restriction>
2141       </xs:complexContent>
2142     </xs:complexType>
2143
2144     <xs:element name="Identification" type="IdentificationType"/>
2145
2146     <xs:complexType name="IdentificationType">
2147       <xs:complexContent>
2148         <xs:restriction base="ac:IdentificationType">
2149           <xs:sequence>
2150             <xs:element ref="ac:PhysicalVerification"/>
2151             <xs:element ref="ac:WrittenConsent"/>
2152             <xs:element ref="ac:GoverningAgreements"/>

```

```

2153     <xs:element ref="ac:Extension" minOccurs="0"
2154     maxOccurs="unbounded"/>
2155   </xs:sequence>
2156   <xs:attribute name="nym">
2157     <xs:simpleType>
2158       <xs:restriction base="xs:NMTOKEN">
2159         <xs:enumeration value="anonymity"/>
2160         <xs:enumeration value="verinymity"/>
2161         <xs:enumeration value="pseudonymity"/>
2162       </xs:restriction>
2163     </xs:simpleType>
2164   </xs:attribute>
2165 </xs:restriction>
2166 </xs:complexContent>
2167 </xs:complexType>
2168
2169 </xs:schema>

```

2170 3.4.7 MobileTwoFactorContract

2171 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract (

2172 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2173 schema document [SAMLAC-MTFC]).

2174 Reflects mobile contract customer registration procedures and a two-factor based authentication. For
 2175 example, a digital signing device with tamper resistant memory for key storage, such as a GSM SIM, that
 2176 requires explicit proof of user identity and intent, such as a PIN or biometric.

```

2177 <?xml version="1.0" encoding="UTF-8"?>
2178
2179 <xs:schema
2180   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorCo
2181   ntract"
2182   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2183   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2184   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
2185   finalDefault="extension">
2186
2187   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2188   schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2189
2190   <xs:annotation>
2191     <xs:documentation>
2192       urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
2193     </xs:documentation>
2194   </xs:annotation>
2195
2196   <xs:complexType name="AuthnContextDeclaration">
2197     <xs:complexContent>
2198       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2199         <xs:sequence>
2200           <xs:element ref="Identification" minOccurs="0"/>
2201           <xs:element ref="TechnicalProtection" minOccurs="0"/>
2202           <xs:element ref="OperationalProtection" minOccurs="0"/>
2203           <xs:element ref="AuthnMethod"/>
2204           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2205           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
2206             maxOccurs="unbounded"/>
2207           <xs:element ref="ac:Extension" minOccurs="0"
2208             maxOccurs="unbounded"/>
2209         </xs:sequence>
2210         <xs:attribute name="ID" type="xs:ID"/>
2211       </xs:restriction>
2212     </xs:complexContent>
2213   </xs:complexType>

```



```

2214 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2215
2216
2217 <xs:complexType name="AuthnMethodType">
2218   <xs:complexContent>
2219     <xs:restriction base="ac:AuthnMethodBaseType">
2220       <xs:sequence>
2221         <xs:element ref="ac:PrincipalAuthenticationMechanism"
2222 minOccurs="0"/>
2223         <xs:element ref="Authenticator"/>
2224         <xs:element ref="AuthenticatorTransportProtocol"
2225 minOccurs="0"/>
2226         <xs:element ref="ac:Extension" minOccurs="0"
2227 maxOccurs="unbounded"/>
2228       </xs:sequence>
2229     </xs:restriction>
2230   </xs:complexContent>
2231 </xs:complexType>
2232
2233 <xs:element name="Authenticator" type="AuthenticatorType"/>
2234
2235 <xs:complexType name="AuthenticatorType">
2236   <xs:complexContent>
2237     <xs:restriction base="ac:AuthenticatorBaseType">
2238       <xs:choice>
2239         <xs:element ref="ac:DigSig"/>
2240         <xs:element ref="ac:ZeroKnowledge"/>
2241         <xs:element ref="ac:SharedSecretChallengeResponse"/>
2242         <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
2243         <xs:element ref="ac:AsymmetricDecryption"/>
2244         <xs:element ref="ac:AsymmetricKeyAgreement"/>
2245       <xs:sequence>
2246         <xs:element ref="ac:Password" minOccurs="1"/>
2247       <xs:choice>
2248         <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
2249         <xs:element ref="ac:SharedSecretChallengeResponse"/>
2250       </xs:choice>
2251       <xs:element ref="ac:Extension" maxOccurs="unbounded"/>
2252     </xs:sequence>
2253   </xs:choice>
2254 </xs:restriction>
2255 </xs:complexContent>
2256 </xs:complexType>
2257
2258 <xs:element name="AuthenticatorTransportProtocol"
2259 type="SecureTransportType"/>
2260
2261 <xs:complexType name="SecureTransportType">
2262   <xs:complexContent>
2263     <xs:restriction base="ac:AuthenticatorTransportProtocolType">
2264       <xs:choice>
2265         <xs:element ref="ac:SSL"/>
2266         <xs:element ref="ac:MobileNetworkNoEncryption"/>
2267         <xs:element ref="ac:MobileNetworkRadioEncryption"/>
2268         <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
2269         <xs:element ref="ac:WTLS"/>
2270       </xs:choice>
2271     </xs:restriction>
2272   </xs:complexContent>
2273 </xs:complexType>
2274
2275 <xs:element name="OperationalProtection"
2276 type="OperationalProtectionType"/>
2277
2278 <xs:complexType name="OperationalProtectionType">
2279   <xs:complexContent>
2280     <xs:restriction base="OperationalProtectionType">

```

```

2281         <xs:sequence>
2282             <xs:element ref="ac:SecurityAudit"/>
2283             <xs:element ref="ac:DeactivationCallCenter"/>
2284             <xs:element ref="ac:Extension" minOccurs="0"
2285 maxOccurs="unbounded"/>
2286         </xs:sequence>
2287     </xs:restriction>
2288 </xs:complexContent>
2289 </xs:complexType>
2290
2291 <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
2292
2293 <xs:complexType name="TechnicalProtectionType">
2294     <xs:complexContent>
2295         <xs:restriction base="ac:TechnicalProtectionBaseType">
2296             <xs:choice>
2297                 <xs:element ref="PrivateKeyProtection"/>
2298                 <xs:element ref="SecretKeyProtection"/>
2299             </xs:choice>
2300         </xs:restriction>
2301     </xs:complexContent>
2302 </xs:complexType>
2303
2304 <xs:element name="PrivateKeyProtection"
2305 type="PrivateKeyProtectionType"/>
2306
2307 <xs:complexType name="PrivateKeyProtectionType">
2308     <xs:complexContent>
2309         <xs:restriction base="ac:PrivateKeyProtectionType">
2310             <xs:sequence>
2311                 <xs:element ref="KeyActivation"/>
2312                 <xs:element ref="KeyStorage"/>
2313                 <xs:element ref="ac:Extension" minOccurs="0"
2314 maxOccurs="unbounded"/>
2315             </xs:sequence>
2316         </xs:restriction>
2317     </xs:complexContent>
2318 </xs:complexType>
2319
2320 <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>
2321
2322 <xs:complexType name="SecretKeyProtectionType">
2323     <xs:complexContent>
2324         <xs:restriction base="ac:SecretKeyProtectionType">
2325             <xs:sequence>
2326                 <xs:element ref="KeyActivation"/>
2327                 <xs:element ref="KeyStorage"/>
2328                 <xs:element ref="ac:Extension" minOccurs="0"
2329 maxOccurs="unbounded"/>
2330             </xs:sequence>
2331         </xs:restriction>
2332     </xs:complexContent>
2333 </xs:complexType>
2334
2335 <xs:element name="KeyActivation" type="KeyActivationType"/>
2336
2337 <xs:complexType name="KeyActivationType">
2338     <xs:complexContent>
2339         <xs:restriction base="ac:KeyActivationType">
2340             <xs:sequence>
2341                 <xs:element ref="ac:ActivationPin"/>
2342                 <xs:element ref="ac:Extension" minOccurs="0"
2343 maxOccurs="unbounded"/>
2344             </xs:sequence>
2345         </xs:restriction>
2346     </xs:complexContent>
2347 </xs:complexType>

```

```

2348
2349 <xs:element name="KeyStorage" type="KeyStorageType"/>
2350
2351 <xs:complexType name="KeyStorageType">
2352   <xs:complexContent>
2353     <xs:restriction base="ac:KeyStorageType">
2354       <xs:attribute name="medium" use="required">
2355         <xs:simpleType>
2356           <xs:restriction base="xs:NMTOKEN">
2357             <xs:enumeration value="MobileDevice"/>
2358             <xs:enumeration value="MobileAuthCard"/>
2359             <xs:enumeration value="smartcard"/>
2360           </xs:restriction>
2361         </xs:simpleType>
2362       </xs:attribute>
2363     </xs:restriction>
2364   </xs:complexContent>
2365 </xs:complexType>
2366
2367 <xs:element name="SecurityAudit" type="SecurityAuditType"/>
2368
2369 <xs:complexType name="SecurityAuditType">
2370   <xs:complexContent>
2371     <xs:restriction base="ac:SecurityAuditType">
2372       <xs:sequence>
2373         <xs:element ref="ac:SwitchAudit"/>
2374         <xs:element ref="ac:Extension" minOccurs="0"
2375 maxOccurs="unbounded"/>
2376       </xs:sequence>
2377     </xs:restriction>
2378   </xs:complexContent>
2379 </xs:complexType>
2380
2381 <xs:element name="Identification" type="IdentificationType"/>
2382
2383 <xs:complexType name="IdentificationType">
2384   <xs:complexContent>
2385     <xs:restriction base="ac:IdentificationType">
2386       <xs:sequence>
2387         <xs:element ref="ac:PhysicalVerification"/>
2388         <xs:element ref="ac:WrittenConsent"/>
2389         <xs:element ref="ac:GoverningAgreements"/>
2390         <xs:element ref="ac:Extension" minOccurs="0"
2391 maxOccurs="unbounded"/>
2392       </xs:sequence>
2393       <xs:attribute name="nym">
2394         <xs:simpleType>
2395           <xs:restriction base="xs:NMTOKEN">
2396             <xs:enumeration value="anonymity"/>
2397             <xs:enumeration value="verinymity"/>
2398             <xs:enumeration value="pseudonymity"/>
2399           </xs:restriction>
2400         </xs:simpleType>
2401       </xs:attribute>
2402     </xs:restriction>
2403   </xs:complexContent>
2404 </xs:complexType>
2405
2406 </xs:schema>

```

2407 3.4.8 Password

2408 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Password

2409 Note that this URI is also used as the target namespace in the corresponding authentication context class
2410 schema document [SAMLAC-Pass]).

2411 The Password class is identified when a Principal authenticates to an authentication authority through the
2412 presentation of a password over an unprotected HTTP session.

```
2413 <?xml version="1.0" encoding="UTF-8"?>
2414
2415 <xs:schema
2416 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
2417 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2418 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2419 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
2420 finalDefault="extension">
2421
2422   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2423   schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2424
2425   <xs:annotation>
2426     <xs:documentation>
2427       urn:oasis:names:tc:SAML:2.0:ac:classes:Password
2428     </xs:documentation>
2429   </xs:annotation>
2430
2431   <xs:complexType name="AuthnContextDeclaration">
2432     <xs:complexContent>
2433       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2434         <xs:sequence>
2435           <xs:element ref="ac:Identification" minOccurs="0"/>
2436           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2437           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
2438           <xs:element ref="AuthnMethod"/>
2439           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2440           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
2441             maxOccurs="unbounded"/>
2442           <xs:element ref="ac:Extension" minOccurs="0"
2443             maxOccurs="unbounded"/>
2444         </xs:sequence>
2445         <xs:attribute name="ID" type="xs:ID"/>
2446       </xs:restriction>
2447     </xs:complexContent>
2448   </xs:complexType>
2449
2450   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2451
2452   <xs:complexType name="AuthnMethodType">
2453     <xs:complexContent>
2454       <xs:restriction base="ac:AuthnMethodBaseType">
2455         <xs:sequence>
2456           <xs:element ref="ac:PrincipalAuthenticationMechanism"
2457             minOccurs="0"/>
2458           <xs:element ref="Authenticator"/>
2459           <xs:element ref="ac:AuthenticatorTransportProtocol"
2460             minOccurs="0"/>
2461           <xs:element ref="ac:Extension" minOccurs="0"
2462             maxOccurs="unbounded"/>
2463         </xs:sequence>
2464       </xs:restriction>
2465     </xs:complexContent>
2466   </xs:complexType>
2467
2468   <xs:element name="Authenticator" type="AuthenticatorType"/>
2469
2470   <xs:complexType name="AuthenticatorType">
2471     <xs:complexContent>
2472       <xs:restriction base="ac:AuthenticatorBaseType">
2473         <xs:choice>
2474           <xs:element ref="ac:RestrictedPassword"/>
2475         </xs:choice>
2476       </xs:restriction>

```

```
2477     </xs:complexContent>
2478   </xs:complexType>
2479
2480 </xs:schema>
```

2481 Following is an example of an XML instance that conforms to the context class schema:

```
2482 <?xml version="1.0" encoding="UTF-8"?>
2483
2484   <AuthenticationContextDeclaration
2485     xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2486     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
2487     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password">
2488
2489     <AuthnMethod>
2490       <Authenticator>
2491         <ac:RestrictedPassword>
2492           <ac:RestrictedLength min="4"/>
2493         </ac:RestrictedPassword>
2494       </Authenticator>
2495     </AuthnMethod>
2496
2497   </AuthenticationContextDeclaration>
```

2498 3.4.9 PasswordProtectedTransport

2499 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

2500 Note that this URI is also used as the target namespace in the corresponding authentication context class
2501 schema document [SAMLAC-PPT]).

2502 The PasswordProtectedTransport class is identified when a Principal authenticates to an authentication
2503 authority through the presentation of a password over a protected session.

```
2504 <?xml version="1.0" encoding="UTF-8"?>
2505
2506 <xs:schema
2507   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected
2508   Transport"
2509   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2510   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2511   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
2512   finalDefault="extension">
2513
2514   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2515   schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2516
2517   <xs:annotation>
2518     <xs:documentation>
2519       urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
2520     </xs:documentation>
2521   </xs:annotation>
2522
2523   <xs:complexType name="AuthnContextDeclaration">
2524     <xs:complexContent>
2525       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2526         <xs:sequence>
2527           <xs:element ref="ac:Identification" minOccurs="0"/>
2528           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2529           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
2530           <xs:element ref="AuthnMethod"/>
2531           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2532           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
2533             maxOccurs="unbounded"/>
2534           <xs:element ref="ac:Extension" minOccurs="0"
2535             maxOccurs="unbounded"/>
2536         </xs:sequence>
2537       </xs:restriction>
2538     </xs:complexContent>
2539   </xs:complexType>
```

```

2537         </xs:sequence>
2538         <xs:attribute name="ID" type="xs:ID"/>
2539     </xs:restriction>
2540 </xs:complexContent>
2541 </xs:complexType>
2542
2543 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2544
2545 <xs:complexType name="AuthnMethodType">
2546     <xs:complexContent>
2547         <xs:restriction base="ac:AuthnMethodBaseType">
2548             <xs:sequence>
2549                 <xs:element ref="ac:PrincipalAuthenticationMechanism"
2550 minOccurs="0"/>
2551                 <xs:element ref="Authenticator"/>
2552                 <xs:element ref="AuthenticatorTransportProtocol"/>
2553                 <xs:element ref="ac:Extension" minOccurs="0"
2554 maxOccurs="unbounded"/>
2555             </xs:sequence>
2556         </xs:restriction>
2557     </xs:complexContent>
2558 </xs:complexType>
2559
2560 <xs:element name="Authenticator" type="AuthenticatorType"/>
2561
2562 <xs:complexType name="AuthenticatorType">
2563     <xs:complexContent>
2564         <xs:restriction base="ac:AuthenticatorBaseType">
2565             <xs:choice>
2566                 <xs:element ref="ac:RestrictedPassword"/>
2567             </xs:choice>
2568         </xs:restriction>
2569     </xs:complexContent>
2570 </xs:complexType>
2571
2572 <xs:element name="AuthenticatorTransportProtocol"
2573 type="SecureTransportType"/>
2574
2575 <xs:complexType name="SecureTransportType">
2576     <xs:complexContent>
2577         <xs:restriction base="ac:AuthenticatorTransportProtocolType">
2578             <xs:choice>
2579                 <xs:element ref="ac:SSL"/>
2580                 <xs:element ref="ac:MobileNetworkRadioEncryption"/>
2581                 <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
2582                 <xs:element ref="ac:WTLS"/>
2583                 <xs:element ref="ac:IPSec"/>
2584             </xs:choice>
2585         </xs:restriction>
2586     </xs:complexContent>
2587 </xs:complexType>
2588
2589 </xs:schema>

```

2590 **3.4.10 PreviousSession**

2591 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession

2592 Note that this URI is also used as the target namespace in the corresponding authentication context class
2593 schema document [SAMLAC-Prev]).

2594 The PreviousSession class is identified when a Principal had authenticated to an authentication authority
2595 at some point in the past using any authentication context supported by that authentication authority.
2596 Consequently, a subsequent authentication event that the authentication authority will assert to the service
2597 provider may be significantly separated in time from the Principals current resource access request.

2598 The context for the previously authenticated session is explicitly not included in this context class because
2599 the user has not authenticated during this session, and so the mechanism that the user employed to
2600 authenticate in a previous session should not be used as part of a decision on whether to now allow
2601 access to a resource.

```
2602 <?xml version="1.0" encoding="UTF-8"?>
2603
2604 <xs:schema
2605 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2606 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2607 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2608 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2609 finalDefault="extension">
2610
2611   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2612 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2613
2614   <xs:annotation>
2615     <xs:documentation>
2616       urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
2617     </xs:documentation>
2618   </xs:annotation>
2619
2620   <xs:complexType name="AuthnContextDeclaration">
2621     <xs:complexContent>
2622       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2623         <xs:sequence>
2624           <xs:element ref="ac:Identification" minOccurs="0"/>
2625           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2626           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
2627           <xs:element ref="AuthnMethod"/>
2628           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2629           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
2630             maxOccurs="unbounded"/>
2631           <xs:element ref="ac:Extension" minOccurs="0"
2632             maxOccurs="unbounded"/>
2633         </xs:sequence>
2634         <xs:attribute name="ID" type="xs:ID"/>
2635       </xs:restriction>
2636     </xs:complexContent>
2637   </xs:complexType>
2638
2639   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2640
2641   <xs:complexType name="AuthnMethodType">
2642     <xs:complexContent>
2643       <xs:restriction base="ac:AuthnMethodBaseType">
2644         <xs:sequence>
2645           <xs:element ref="ac:PrincipalAuthenticationMechanism"
2646 minOccurs="0"/>
2647           <xs:element ref="Authenticator"/>
2648           <xs:element ref="ac:AuthenticatorTransportProtocol"
2649             minOccurs="0"/>
2650           <xs:element ref="ac:Extension" minOccurs="0"
2651             maxOccurs="unbounded"/>
2652         </xs:sequence>
2653       </xs:restriction>
2654     </xs:complexContent>
2655   </xs:complexType>
2656
2657   <xs:element name="Authenticator" type="PreviousSessionType"/>
2658
2659   <xs:complexType name="PreviousSessionType">
2660     <xs:complexContent>
2661       <xs:restriction base="ac:AuthenticatorBaseType">
2662         <xs:choice>
2663           <xs:element ref="ac:PreviousSession"/>
```

```
2664     </xs:choice>
2665     </xs:restriction>
2666     </xs:complexContent>
2667   </xs:complexType>
2668
2669 </xs:schema>
```

2670 **3.4.11 Public Key – X.509**

2671 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:X509

2672 Note that this URI is also used as the target namespace in the corresponding authentication context class
2673 schema document [SAMLAC-X509]).

2674 The X509 context class indicates that the Principal authenticated by means of a digital signature where
2675 the key was validated as part of an X.509 Public Key Infrastructure.

```
2676 <?xml version="1.0" encoding="UTF-8"?>
2677
2678 <xs:schema
2679   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2680   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2681   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2682   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2683   finalDefault="extension">
2684
2685   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2686     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2687
2688   <xs:annotation>
2689     <xs:documentation>
2690       urn:oasis:names:tc:SAML:2.0:ac:classes:X509
2691     </xs:documentation>
2692   </xs:annotation>
2693
2694   <xs:complexType name="AuthnContextDeclaration">
2695     <xs:complexContent>
2696       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2697         <xs:sequence>
2698           <xs:element ref="ac:Identification" minOccurs="0"/>
2699           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2700           <xs:element ref="ac:OperationalProtection"
2701             minOccurs="0"/>
2702           <xs:element ref="AuthnMethod"/>
2703           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2704           <xs:element ref="ac:AuthenticatingAuthority"
2705             minOccurs="0"
2706             maxOccurs="unbounded"/>
2707           <xs:element ref="ac:Extension" minOccurs="0"
2708             maxOccurs="unbounded"/>
2709         </xs:sequence>
2710         <xs:attribute name="ID" type="xs:ID"/>
2711       </xs:restriction>
2712     </xs:complexContent>
2713   </xs:complexType>
2714
2715   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2716
2717   <xs:complexType name="AuthnMethodType">
2718     <xs:complexContent>
2719       <xs:restriction base="ac:AuthnMethodBaseType">
2720         <xs:sequence>
```



```

2721     <xs:element ref="AuthnMechanism"/>
2722     <xs:element ref="Authenticator"/>
2723     <xs:element ref="ac:AuthenticatorTransportProtocol"
2724         minOccurs="0"/>
2725     <xs:element ref="ac:Extension" minOccurs="0"
2726         maxOccurs="unbounded"/>
2727     </xs:sequence>
2728 </xs:restriction>
2729 </xs:complexContent>
2730 </xs:complexType>
2731
2732     <xs:element name="AuthnMechanism"
2733 type="PasswordAuthnMechanismType"/>
2734
2735     <xs:complexType name="PasswordAuthnMechanismType">
2736     <xs:complexContent>
2737     <xs:restriction
2738 base="ac:PrincipalAuthenticationMechanismType">
2739     <xs:sequence>
2740     <xs:choice>
2741     <xs:element ref="ac:RestrictedPassword"/>
2742     </xs:choice>
2743     </xs:sequence>
2744     <xs:attribute name="preauth" type="xs:integer"
2745 use="optional"/>
2746     </xs:restriction>
2747 </xs:complexContent>
2748 </xs:complexType>
2749
2750 <xs:element name="Authenticator" type="AuthenticatorType"/>
2751
2752 <xs:complexType name="AuthenticatorType">
2753 <xs:complexContent>
2754 <xs:restriction base="ac:AuthenticatorBaseType">
2755 <xs:choice>
2756 <xs:element ref="DigSig"/>
2757 </xs:choice>
2758 </xs:restriction>
2759 </xs:complexContent>
2760 </xs:complexType>
2761
2762 <xs:element name="DigSig" type="DigSigType"/>
2763
2764 <xs:complexType name="DigSigType">
2765 <xs:complexContent>
2766 <xs:restriction base="ac:PublicKeyType">
2767 <xs:attribute name="keyValidation"
2768 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
2769 </xs:restriction>
2770 </xs:complexContent>
2771 </xs:complexType>
2772
2773 </xs:schema>

```

2774 3.4.12 Public Key – PGP

2775 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PGP

2776 Note that this URI is also used as the target namespace in the corresponding authentication context class
2777 schema document [SAMLAC-PGP]).

2778 The PGP context class indicates that the Principal authenticated by means of a digital signature where the
2779 key was validated as part of a PGP Public Key Infrastructure.

```
2780 <?xml version="1.0" encoding="UTF-8"?>
2781
2782 <xs:schema
2783 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
2784 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2785 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2786 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
2787 finalDefault="extension">
2788
2789   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2790 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2791
2792   <xs:annotation>
2793     <xs:documentation>
2794       urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
2795     </xs:documentation>
2796   </xs:annotation>
2797
2798   <xs:complexType name="AuthnContextDeclaration">
2799     <xs:complexContent>
2800       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2801         <xs:sequence>
2802           <xs:element ref="ac:Identification" minOccurs="0"/>
2803           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2804           <xs:element ref="ac:OperationalProtection"
2805 minOccurs="0"/>
2806           <xs:element ref="AuthnMethod"/>
2807           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2808           <xs:element ref="ac:AuthenticatingAuthority"
2809 minOccurs="0"
2810 maxOccurs="unbounded"/>
2811           <xs:element ref="ac:Extension" minOccurs="0"
2812 maxOccurs="unbounded"/>
2813         </xs:sequence>
2814         <xs:attribute name="ID" type="xs:ID"/>
2815       </xs:restriction>
2816     </xs:complexContent>
2817   </xs:complexType>
2818
2819   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2820
2821   <xs:complexType name="AuthnMethodType">
2822     <xs:complexContent>
2823       <xs:restriction base="ac:AuthnMethodBaseType">
2824         <xs:sequence>
2825           <xs:element ref="AuthnMechanism"/>
2826           <xs:element ref="Authenticator"/>
2827           <xs:element ref="ac:AuthenticatorTransportProtocol"
2828 minOccurs="0"/>
2829           <xs:element ref="ac:Extension" minOccurs="0"
2830 maxOccurs="unbounded"/>
2831         </xs:sequence>
2832       </xs:restriction>
2833     </xs:complexContent>
2834   </xs:complexType>
2835
2836   <xs:element name="AuthnMechanism"
2837 type="PasswordAuthnMechanismType"/>
2838
```

```

2839     <xs:complexType name="PasswordAuthnMechanismType">
2840       <xs:complexContent>
2841         <xs:restriction
2842 base="ac:PrincipalAuthenticationMechanismType">
2843           <xs:sequence>
2844             <xs:choice>
2845               <xs:element ref="ac:RestrictedPassword"/>
2846             </xs:choice>
2847           </xs:sequence>
2848           <xs:attribute name="preauth" type="xs:integer"
2849 use="optional"/>
2850         </xs:restriction>
2851       </xs:complexContent>
2852     </xs:complexType>
2853
2854     <xs:element name="Authenticator" type="AuthenticatorType"/>
2855
2856     <xs:complexType name="AuthenticatorType">
2857       <xs:complexContent>
2858         <xs:restriction base="ac:AuthenticatorBaseType">
2859           <xs:choice>
2860             <xs:element ref="DigSig"/>
2861           </xs:choice>
2862         </xs:restriction>
2863       </xs:complexContent>
2864     </xs:complexType>
2865
2866     <xs:element name="DigSig" type="DigSigType"/>
2867
2868     <xs:complexType name="DigSigType">
2869       <xs:complexContent>
2870         <xs:restriction base="ac:PublicKeyType">
2871           <xs:attribute name="keyValidation"
2872 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
2873         </xs:restriction>
2874       </xs:complexContent>
2875     </xs:complexType>
2876
2877 </xs:schema>

```

2878 **3.4.13 Public Key – SPKI**

2879 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI

2880 Note that this URI is also used as the target namespace in the corresponding authentication context class
2881 schema document [SAMLAC-SPKI]).

2882 The SPKI context class indicates that the Principal authenticated by means of a digital signature where
2883 the key was validated via an SPKI Infrastructure.

```

2884 <?xml version="1.0" encoding="UTF-8"?>
2885
2886 <xs:schema
2887 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2888 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2889 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2890 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2891 finalDefault="extension">
2892
2893   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2894 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

```

```

2895
2896     <xs:annotation>
2897       <xs:documentation>
2898         urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
2899       </xs:documentation>
2900     </xs:annotation>
2901
2902     <xs:complexType name="AuthnContextDeclaration">
2903       <xs:complexContent>
2904         <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2905           <xs:sequence>
2906             <xs:element ref="ac:Identification" minOccurs="0"/>
2907             <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2908             <xs:element ref="ac:OperationalProtection"
2909 minOccurs="0"/>
2910             <xs:element ref="AuthnMethod"/>
2911             <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2912             <xs:element ref="ac:AuthenticatingAuthority"
2913 minOccurs="0"
2914             maxOccurs="unbounded"/>
2915             <xs:element ref="ac:Extension" minOccurs="0"
2916             maxOccurs="unbounded"/>
2917           </xs:sequence>
2918           <xs:attribute name="ID" type="xs:ID"/>
2919         </xs:restriction>
2920       </xs:complexContent>
2921     </xs:complexType>
2922
2923     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2924
2925     <xs:complexType name="AuthnMethodType">
2926       <xs:complexContent>
2927         <xs:restriction base="ac:AuthnMethodBaseType">
2928           <xs:sequence>
2929             <xs:element ref="AuthnMechanism"/>
2930             <xs:element ref="Authenticator"/>
2931             <xs:element ref="ac:AuthenticatorTransportProtocol"
2932             minOccurs="0"/>
2933             <xs:element ref="ac:Extension" minOccurs="0"
2934             maxOccurs="unbounded"/>
2935           </xs:sequence>
2936         </xs:restriction>
2937       </xs:complexContent>
2938     </xs:complexType>
2939
2940     <xs:element name="AuthnMechanism"
2941 type="PasswordAuthnMechanismType"/>
2942
2943     <xs:complexType name="PasswordAuthnMechanismType">
2944       <xs:complexContent>
2945         <xs:restriction
2946 base="ac:PrincipalAuthenticationMechanismType">
2947           <xs:sequence>
2948             <xs:choice>
2949               <xs:element ref="ac:RestrictedPassword"/>
2950             </xs:choice>
2951           </xs:sequence>
2952           <xs:attribute name="preauth" type="xs:integer"
2953 use="optional"/>
2954         </xs:restriction>
2955       </xs:complexContent>

```

```

2956 </xs:complexType>
2957
2958 <xs:element name="Authenticator" type="AuthenticatorType"/>
2959
2960 <xs:complexType name="AuthenticatorType">
2961   <xs:complexContent>
2962     <xs:restriction base="ac:AuthenticatorBaseType">
2963       <xs:choice>
2964         <xs:element ref="DigSig"/>
2965       </xs:choice>
2966     </xs:restriction>
2967   </xs:complexContent>
2968 </xs:complexType>
2969
2970 <xs:element name="DigSig" type="DigSigType"/>
2971
2972 <xs:complexType name="DigSigType">
2973   <xs:complexContent>
2974     <xs:restriction base="ac:PublicKeyType">
2975       <xs:attribute name="keyValidation"
2976 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
2977     </xs:restriction>
2978   </xs:complexContent>
2979 </xs:complexType>
2980
2981 </xs:schema>

```

2982 3.4.14 Public Key - XML Digital Signature

2983 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig

2984 Note that this URI is also used as the target namespace in the corresponding authentication context class
 2985 schema document [SAMLAC-X509]).

2986 This context class indicates that the Principal authenticated by means of a digital signature according to
 2987 the processing rules specified in the XML Digital Signature specification [XMLSig].

```

2988 <?xml version="1.0" encoding="UTF-8"?>
2989
2990 <xs:schema
2991 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
2992 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2993 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2994 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
2995 finalDefault="extension">
2996
2997   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2998 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2999
3000   <xs:annotation>
3001     <xs:documentation>
3002       urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
3003     </xs:documentation>
3004   </xs:annotation>
3005
3006   <xs:complexType name="AuthnContextDeclaration">
3007     <xs:complexContent>
3008       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3009         <xs:sequence>
3010           <xs:element ref="ac:Identification" minOccurs="0"/>
3011           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>

```

```

3012         <xs:element ref="ac:OperationalProtection"
3013 minOccurs="0"/>
3014         <xs:element ref="AuthnMethod"/>
3015         <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3016         <xs:element ref="ac:AuthenticatingAuthority"
3017 minOccurs="0"
3018             maxOccurs="unbounded"/>
3019         <xs:element ref="ac:Extension" minOccurs="0"
3020             maxOccurs="unbounded"/>
3021     </xs:sequence>
3022     <xs:attribute name="ID" type="xs:ID"/>
3023 </xs:restriction>
3024 </xs:complexContent>
3025 </xs:complexType>
3026
3027 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3028
3029 <xs:complexType name="AuthnMethodType">
3030     <xs:complexContent>
3031         <xs:restriction base="ac:AuthnMethodBaseType">
3032             <xs:sequence>
3033                 <xs:element ref="AuthnMechanism"/>
3034                 <xs:element ref="Authenticator"/>
3035                 <xs:element ref="ac:AuthenticatorTransportProtocol"
3036                     minOccurs="0"/>
3037                 <xs:element ref="ac:Extension" minOccurs="0"
3038                     maxOccurs="unbounded"/>
3039             </xs:sequence>
3040         </xs:restriction>
3041     </xs:complexContent>
3042 </xs:complexType>
3043
3044     <xs:element name="AuthnMechanism"
3045 type="PasswordAuthnMechanismType"/>
3046
3047     <xs:complexType name="PasswordAuthnMechanismType">
3048         <xs:complexContent>
3049             <xs:restriction
3050 base="ac:PrincipalAuthenticationMechanismType">
3051                 <xs:sequence>
3052                     <xs:choice>
3053                         <xs:element ref="ac:RestrictedPassword"/>
3054                     </xs:choice>
3055                 </xs:sequence>
3056                 <xs:attribute name="preauth" type="xs:integer"
3057 use="optional"/>
3058             </xs:restriction>
3059         </xs:complexContent>
3060     </xs:complexType>
3061
3062 <xs:element name="Authenticator" type="AuthenticatorType"/>
3063
3064 <xs:complexType name="AuthenticatorType">
3065     <xs:complexContent>
3066         <xs:restriction base="ac:AuthenticatorBaseType">
3067             <xs:choice>
3068                 <xs:element ref="DigSig"/>
3069             </xs:choice>
3070         </xs:restriction>
3071     </xs:complexContent>
3072 </xs:complexType>

```

```

3073
3074     <xs:element name="DigSig" type="DigSigType"/>
3075
3076     <xs:complexType name="DigSigType">
3077         <xs:complexContent>
3078             <xs:restriction base="ac:PublicKeyType">
3079                 <xs:attribute name="keyValidation"
3080 fixed="urn:ietf:rfc:3075"/>
3081             </xs:restriction>
3082         </xs:complexContent>
3083     </xs:complexType>
3084
3085 </xs:schema>

```

3086 **3.4.15 Smartcard**

3087 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard

3088 Note that this URI is also used as the target namespace in the corresponding authentication context class
3089 schema document [SAMLAC-Smart].

3090 The Smartcard class is identified when a Principal authenticates to an authentication authority using a
3091 smartcard.

```

3092 <?xml version="1.0" encoding="UTF-8"?>
3093
3094 <xs:schema
3095 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
3096 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3097 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3098 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
3099 finalDefault="extension">
3100
3101     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3102 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3103
3104     <xs:annotation>
3105         <xs:documentation>
3106             urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
3107         </xs:documentation>
3108     </xs:annotation>
3109
3110     <xs:complexType name="AuthnContextDeclaration">
3111         <xs:complexContent>
3112             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3113                 <xs:sequence>
3114                     <xs:element ref="ac:Identification" minOccurs="0"/>
3115                     <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3116                     <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3117                     <xs:element ref="AuthnMethod"/>
3118                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3119                     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3120 maxOccurs="unbounded"/>
3121                     <xs:element ref="ac:Extension" minOccurs="0"
3122 maxOccurs="unbounded"/>
3123                 </xs:sequence>
3124                 <xs:attribute name="ID" type="xs:ID"/>
3125             </xs:restriction>
3126         </xs:complexContent>
3127     </xs:complexType>
3128
3129     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3130
3131     <xs:complexType name="AuthnMethodType">
3132         <xs:complexContent>

```

```

3133     <xs:restriction base="ac:AuthnMethodBaseType">
3134         <xs:sequence>
3135             <xs:element ref="AuthnMechanism"/>
3136             <xs:element ref="ac:Authenticator"/>
3137             <xs:element ref="ac:AuthenticatorTransportProtocol"
3138                 minOccurs="0"/>
3139             <xs:element ref="ac:Extension" minOccurs="0"
3140                 maxOccurs="unbounded"/>
3141         </xs:sequence>
3142     </xs:restriction>
3143 </xs:complexContent>
3144 </xs:complexType>
3145
3146 <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>
3147
3148 <xs:complexType name="SmartcardAuthnMechanismType">
3149     <xs:complexContent>
3150         <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
3151             <xs:sequence>
3152                 <xs:choice>
3153                     <xs:element ref="ac:Smartcard"/>
3154                 </xs:choice>
3155             </xs:sequence>
3156         </xs:restriction>
3157     </xs:complexContent>
3158 </xs:complexType>
3159
3160 </xs:schema>

```

3161 3.4.16 SmartcardPKI

3162 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

3163 Note that this URI is also used as the target namespace in the corresponding authentication context class
3164 schema document [SAMLAC-SmPKI]).

3165 The SmartcardPKI class is identified when a Principal authenticates to an authentication authority through
3166 a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN.

```

3167 <?xml version="1.0" encoding="UTF-8"?>
3168
3169 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
3170     xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3171     xmlns:xs="http://www.w3.org/2001/XMLSchema"
3172     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
3173     finalDefault="extension">
3174
3175     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac" schemaLocation="sstc-saml-
3176 schema-authn-context-1.0.xsd"/>
3177
3178     <xs:annotation>
3179         <xs:documentation>
3180             urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
3181         </xs:documentation>
3182     </xs:annotation>
3183
3184     <xs:complexType name="AuthnContextDeclaration">
3185         <xs:complexContent>
3186             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3187                 <xs:sequence>
3188                     <xs:element ref="ac:Identification" minOccurs="0"/>
3189                     <xs:element ref="TechnicalProtection"/>
3190                     <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3191                     <xs:element ref="AuthnMethod"/>
3192                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3193                     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"

```



```

3194         maxOccurs="unbounded"/>
3195     <xs:element ref="ac:Extension" minOccurs="0"
3196         maxOccurs="unbounded"/>
3197     </xs:sequence>
3198     <xs:attribute name="ID" type="xs:ID"/>
3199 </xs:restriction>
3200 </xs:complexContent>
3201 </xs:complexType>
3202
3203 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3204
3205 <xs:complexType name="AuthnMethodType">
3206     <xs:complexContent>
3207         <xs:restriction base="ac:AuthnMethodBaseType">
3208             <xs:sequence>
3209                 <xs:element ref="AuthnMechanism"/>
3210                 <xs:element ref="Authenticator"/>
3211                 <xs:element ref="ac:AuthenticatorTransportProtocol"
3212                     minOccurs="0"/>
3213                 <xs:element ref="ac:Extension" minOccurs="0"
3214                     maxOccurs="unbounded"/>
3215             </xs:sequence>
3216         </xs:restriction>
3217     </xs:complexContent>
3218 </xs:complexType>
3219
3220 <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
3221
3222 <xs:complexType name="TechnicalProtectionType">
3223     <xs:complexContent>
3224         <xs:restriction base="ac:TechnicalProtectionBaseType">
3225             <xs:sequence>
3226                 <xs:choice>
3227                     <xs:element ref="PrivateKeyProtection"/>
3228                     <xs:element ref="ac:SecretKeyProtection" minOccurs="0"/>
3229                     <xs:element ref="ac:Extension" minOccurs="0"
3230                         maxOccurs="unbounded"/>
3231                 </xs:choice>
3232             </xs:sequence>
3233         </xs:restriction>
3234     </xs:complexContent>
3235 </xs:complexType>
3236
3237 <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>
3238
3239 <xs:complexType name="SmartcardAuthnMechanismType">
3240     <xs:complexContent>
3241         <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
3242             <xs:sequence>
3243                 <xs:element ref="ac:ActivationPin"/>
3244                 <xs:element ref="ac:Smartcard"/>
3245                 <xs:element ref="ac:Extension" minOccurs="0" maxOccurs="unbounded"/>
3246             </xs:sequence>
3247         </xs:restriction>
3248     </xs:complexContent>
3249 </xs:complexType>
3250
3251 <xs:element name="Authenticator" type="SmartCardPKIAuthenticatorType"/>
3252
3253 <xs:complexType name="SmartCardPKIAuthenticatorType">
3254     <xs:complexContent>
3255         <xs:restriction base="ac:AuthenticatorBaseType">
3256             <xs:choice>
3257                 <xs:element ref="ac:AsymmetricDecryption"/>
3258                 <xs:element ref="ac:AsymmetricKeyAgreement"/>
3259                 <xs:element ref="ac:DigSig"/>
3260             </xs:choice>

```

```

3261     </xs:restriction>
3262   </xs:complexContent>
3263 </xs:complexType>
3264
3265 <xs:element name="PrivateKeyProtection" type="PrivateKeyProtectionType"/>
3266
3267 <xs:complexType name="PrivateKeyProtectionType">
3268   <xs:complexContent>
3269     <xs:restriction base="ac:PrivateKeyProtectionType">
3270       <xs:sequence>
3271         <xs:element ref="KeyActivation"/>
3272         <xs:element ref="KeyStorage"/>
3273         <xs:element ref="ac:Extension" minOccurs="0" maxOccurs="unbounded"/>
3274       </xs:sequence>
3275     </xs:restriction>
3276   </xs:complexContent>
3277 </xs:complexType>
3278
3279 <xs:element name="KeyActivation" type="KeyActivationType"/>
3280
3281 <xs:complexType name="KeyActivationType">
3282   <xs:complexContent>
3283     <xs:restriction base="ac:KeyActivationType">
3284       <xs:choice>
3285         <xs:element ref="ac:ActivationPin"/>
3286       </xs:choice>
3287     </xs:restriction>
3288   </xs:complexContent>
3289 </xs:complexType>
3290
3291 <xs:element name="KeyStorage" type="KeyStorageType"/>
3292
3293 <xs:complexType name="KeyStorageType">
3294   <xs:complexContent>
3295     <xs:restriction base="ac:KeyStorageType">
3296       <xs:attribute name="medium" use="required">
3297         <xs:simpleType>
3298           <xs:restriction base="xs:NMTOKEN">
3299             <xs:enumeration value="smartcard"/>
3300           </xs:restriction>
3301         </xs:simpleType>
3302       </xs:attribute>
3303     </xs:restriction>
3304   </xs:complexContent>
3305 </xs:complexType>
3306
3307 </xs:schema>

```

3308 **3.4.17 SoftwarePKI**

3309 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI

3310 Note that this URI is also used as the target namespace in the corresponding authentication context class
3311 schema document [SAMLAC-SwPKI]).

3312 The Software-PKI class is identified when a Principal uses an X.509 certificate stored in software to
3313 authenticate to the authentication authority.

```

3314     <?xml version="1.0" encoding="UTF-8"?>
3315
3316     <xs:schema
3317       targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3318       xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3319       xmlns:xs="http://www.w3.org/2001/XMLSchema"
3320       xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3321       finalDefault="extension">

```

```

3322
3323     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3324     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3325
3326     <xs:annotation>
3327         <xs:documentation>
3328             urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
3329         </xs:documentation>
3330     </xs:annotation>
3331
3332     <xs:complexType name="AuthnContextDeclaration">
3333         <xs:complexContent>
3334             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3335                 <xs:sequence>
3336                     <xs:element ref="ac:Identification" minOccurs="0"/>
3337                     <xs:element ref="TechnicalProtection"/>
3338                     <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3339                     <xs:element ref="AuthnMethod"/>
3340                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3341                     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3342                         maxOccurs="unbounded"/>
3343                     <xs:element ref="ac:Extension" minOccurs="0"
3344                         maxOccurs="unbounded"/>
3345                 </xs:sequence>
3346                 <xs:attribute name="ID" type="xs:ID"/>
3347             </xs:restriction>
3348         </xs:complexContent>
3349     </xs:complexType>
3350
3351     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3352
3353     <xs:complexType name="AuthnMethodType">
3354         <xs:complexContent>
3355             <xs:restriction base="ac:AuthnMethodBaseType">
3356                 <xs:sequence>
3357                     <xs:element ref="AuthnMechanism"/>
3358                     <xs:element ref="Authenticator"/>
3359                     <xs:element ref="ac:AuthenticatorTransportProtocol"
3360                         minOccurs="0"/>
3361                     <xs:element ref="ac:Extension" minOccurs="0"
3362                         maxOccurs="unbounded"/>
3363                 </xs:sequence>
3364             </xs:restriction>
3365         </xs:complexContent>
3366     </xs:complexType>
3367
3368     <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
3369
3370     <xs:complexType name="TechnicalProtectionType">
3371         <xs:complexContent>
3372             <xs:restriction base="ac:TechnicalProtectionBaseType">
3373                 <xs:sequence>
3374                     <xs:choice>
3375                         <xs:element ref="PrivateKeyProtection"/>
3376                         <xs:element ref="ac:SecretKeyProtection" minOccurs="0"/>
3377                         <xs:element ref="ac:Extension" minOccurs="0"
3378                             maxOccurs="unbounded"/>
3379                     </xs:choice>
3380                 </xs:sequence>
3381             </xs:restriction>
3382         </xs:complexContent>
3383     </xs:complexType>
3384
3385     <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>
3386
3387     <xs:complexType name="SmartcardAuthnMechanismType">
3388         <xs:complexContent>

```

```

3389     <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
3390         <xs:sequence>
3391             <xs:element ref="ac:ActivationPin"/>
3392             <xs:element ref="ac:Extension" minOccurs="0"
3393 maxOccurs="unbounded"/>
3394         </xs:sequence>
3395     </xs:restriction>
3396 </xs:complexContent>
3397 </xs:complexType>
3398
3399 <xs:element name="Authenticator" type="SmartCardPKIAuthenticatorType"/>
3400
3401 <xs:complexType name="SmartCardPKIAuthenticatorType">
3402     <xs:complexContent>
3403         <xs:restriction base="ac:AuthenticatorBaseType">
3404             <xs:choice>
3405                 <xs:element ref="ac:AsymmetricDecryption"/>
3406                 <xs:element ref="ac:AsymmetricKeyAgreement"/>
3407                 <xs:element ref="ac:DigSig"/>
3408             </xs:choice>
3409         </xs:restriction>
3410     </xs:complexContent>
3411 </xs:complexType>
3412
3413 <xs:element name="PrivateKeyProtection"
3414 type="PrivateKeyProtectionType"/>
3415
3416 <xs:complexType name="PrivateKeyProtectionType">
3417     <xs:complexContent>
3418         <xs:restriction base="ac:PrivateKeyProtectionType">
3419             <xs:sequence>
3420                 <xs:element ref="KeyActivation"/>
3421                 <xs:element ref="KeyStorage"/>
3422                 <xs:element ref="ac:Extension" minOccurs="0"
3423 maxOccurs="unbounded"/>
3424             </xs:sequence>
3425         </xs:restriction>
3426     </xs:complexContent>
3427 </xs:complexType>
3428
3429 <xs:element name="KeyActivation" type="KeyActivationType"/>
3430
3431 <xs:complexType name="KeyActivationType">
3432     <xs:complexContent>
3433         <xs:restriction base="ac:KeyActivationType">
3434             <xs:choice>
3435                 <xs:element ref="ac:ActivationPin"/>
3436             </xs:choice>
3437         </xs:restriction>
3438     </xs:complexContent>
3439 </xs:complexType>
3440
3441 <xs:element name="KeyStorage" type="KeyStorageType"/>
3442
3443 <xs:complexType name="KeyStorageType">
3444     <xs:complexContent>
3445         <xs:restriction base="ac:KeyStorageType">
3446             <xs:attribute name="medium" use="required">
3447                 <xs:simpleType>
3448                     <xs:restriction base="xs:NMTOKEN">
3449                         <xs:enumeration value="memory"/>
3450                     </xs:restriction>
3451                 </xs:simpleType>
3452             </xs:attribute>
3453         </xs:restriction>
3454     </xs:complexContent>
3455 </xs:complexType>

```

3456
3457

```
</xs:schema>
```

3458 **3.4.18 Telephony**

3459 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony

3460 Note that this URI is also used as the target namespace in the corresponding authentication context class
3461 schema document [SAMLAC-Tele].

3462 This class is used to indicate that the Principal authenticated via the provision of a fixed-line telephone
3463 number, transported via a telephony protocol such as ADSL.

```
3464 <?xml version="1.0" encoding="UTF-8"?>
3465
3466 <xs:schema
3467 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3468 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3469 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3470 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3471 finalDefault="extension">
3472
3473   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3474 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3475
3476   <xs:annotation>
3477     <xs:documentation>
3478       urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
3479     </xs:documentation>
3480   </xs:annotation>
3481
3482   <xs:complexType name="AuthnContextDeclaration">
3483     <xs:complexContent>
3484       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3485         <xs:sequence>
3486           <xs:element ref="ac:Identification" minOccurs="0"/>
3487           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3488           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3489           <xs:element ref="ac:AuthnMethod"/>
3490           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3491           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3492             maxOccurs="unbounded"/>
3493           <xs:element ref="ac:Extension" minOccurs="0"
3494             maxOccurs="unbounded"/>
3495         </xs:sequence>
3496         <xs:attribute name="ID" type="xs:ID"/>
3497       </xs:restriction>
3498     </xs:complexContent>
3499   </xs:complexType>
3500
3501   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3502
3503   <xs:complexType name="AuthnMethodType">
3504     <xs:complexContent>
3505       <xs:restriction base="ac:AuthnMethodBaseType">
3506         <xs:sequence>
3507           <xs:element ref="ac:PrincipalAuthenticationMechanism"
3508             minOccurs="0"/>
3509           <xs:element ref="Authenticator"/>
3510           <xs:element ref="AuthenticatorTransportProtocol"/>
3511           <xs:element ref="ac:Extension" minOccurs="0"
3512             maxOccurs="unbounded"/>
3513         </xs:sequence>
3514       </xs:restriction>
3515     </xs:complexContent>
3516   </xs:complexType>
```

```

3517
3518     <xs:element name="Authenticator" type="AuthenticatorType"/>
3519
3520     <xs:complexType name="AuthenticatorType">
3521         <xs:complexContent>
3522             <xs:restriction base="ac:AuthenticatorBaseType">
3523                 <xs:choice>
3524                     <xs:element ref="ac:SubscriberLineNumber"/>
3525                 </xs:choice>
3526             </xs:restriction>
3527         </xs:complexContent>
3528     </xs:complexType>
3529
3530     <xs:element name="AuthenticatorTransportProtocol"
3531 type="TransportType"/>
3532
3533     <xs:complexType name="TransportType">
3534         <xs:complexContent>
3535             <xs:restriction base="ac:AuthenticatorTransportProtocolType">
3536                 <xs:choice>
3537                     <xs:element ref="ac:PSTN"/>
3538                     <xs:element ref="ac:ISDN"/>
3539                     <xs:element ref="ac:ADSL"/>
3540                 </xs:choice>
3541             </xs:restriction>
3542         </xs:complexContent>
3543     </xs:complexType>
3544 </xs:schema>
3545

```

3546 **3.4.19 Telephony ("Nomadic")**

3547 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony

3548 Note that this URI is also used as the target namespace in the corresponding authentication context class
3549 schema document [SAMLAC-TNom]).

3550 Indicates that the Principal is "roaming" (perhaps using a phone card) and authenticates via the means of
3551 the line number, a user suffix, and a password element.

```

3552 <?xml version="1.0" encoding="UTF-8"?>
3553
3554 <xs:schema
3555 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3556 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3557 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3558 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3559 finalDefault="extension">
3560
3561     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3562 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3563
3564     <xs:annotation>
3565         <xs:documentation>
3566             urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
3567         </xs:documentation>
3568     </xs:annotation>
3569
3570     <xs:complexType name="AuthnContextDeclaration">
3571         <xs:complexContent>
3572             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3573                 <xs:sequence>
3574                     <xs:element ref="ac:Identification" minOccurs="0"/>
3575                     <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3576                     <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3577                     <xs:element ref="AuthnMethod"/>

```

```

3578     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3579     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3580       maxOccurs="unbounded"/>
3581     <xs:element ref="ac:Extension" minOccurs="0"
3582       maxOccurs="unbounded"/>
3583   </xs:sequence>
3584   <xs:attribute name="ID" type="xs:ID"/>
3585 </xs:restriction>
3586 </xs:complexContent>
3587 </xs:complexType>
3588
3589 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3590
3591 <xs:complexType name="AuthnMethodType">
3592   <xs:complexContent>
3593     <xs:restriction base="ac:AuthnMethodBaseType">
3594       <xs:sequence>
3595         <xs:element ref="ac:PrincipalAuthenticationMechanism"
3596           minOccurs="0"/>
3597         <xs:element ref="Authenticator"/>
3598         <xs:element ref="AuthenticatorTransportProtocol"/>
3599         <xs:element ref="ac:Extension" minOccurs="0"
3600           maxOccurs="unbounded"/>
3601       </xs:sequence>
3602     </xs:restriction>
3603   </xs:complexContent>
3604 </xs:complexType>
3605
3606 <xs:element name="Authenticator" type="AuthenticatorType"/>
3607
3608 <xs:complexType name="AuthenticatorType">
3609   <xs:complexContent>
3610     <xs:restriction base="ac:AuthenticatorBaseType">
3611       <xs:sequence>
3612         <xs:element ref="ac:SubscriberLineNumber"/>
3613         <xs:element ref="ac:UserSuffix"/>
3614         <xs:element ref="ac:Password"/>
3615       </xs:sequence>
3616     </xs:restriction>
3617   </xs:complexContent>
3618 </xs:complexType>
3619
3620 <xs:element name="AuthenticatorTransportProtocol"
3621   type="TransportType"/>
3622
3623 <xs:complexType name="TransportType">
3624   <xs:complexContent>
3625     <xs:restriction base="ac:AuthenticatorTransportProtocolType">
3626       <xs:choice>
3627         <xs:element ref="ac:PSTN"/>
3628         <xs:element ref="ac:ISDN"/>
3629         <xs:element ref="ac:ADSL"/>
3630       </xs:choice>
3631     </xs:restriction>
3632   </xs:complexContent>
3633 </xs:complexType>
3634
3635 </xs:schema>

```

3636 3.4.20 Telephony (Personalized)

3637 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony

3638 Note that this URI is also used as the target namespace in the corresponding authentication context class
3639 schema document [SAMLAC-TPers]).

3640 This class is used to indicate that the Principal authenticated via the provision of a fixed-line telephone
3641 number and a user suffix, transported via a telephony protocol such as ADSL.

```
3642 <?xml version="1.0" encoding="UTF-8"?>
3643
3644 <xs:schema
3645 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelep
3646 hony"
3647 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3648 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3649 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
3650 finalDefault="extension">
3651
3652   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3653 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3654
3655   <xs:annotation>
3656     <xs:documentation>
3657       urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony
3658     </xs:documentation>
3659   </xs:annotation>
3660
3661   <xs:complexType name="AuthnContextDeclaration">
3662     <xs:complexContent>
3663       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3664         <xs:sequence>
3665           <xs:element ref="ac:Identification" minOccurs="0"/>
3666           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3667           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3668           <xs:element ref="AuthnMethod"/>
3669           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3670           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3671             maxOccurs="unbounded"/>
3672           <xs:element ref="ac:Extension" minOccurs="0"
3673             maxOccurs="unbounded"/>
3674         </xs:sequence>
3675         <xs:attribute name="ID" type="xs:ID"/>
3676       </xs:restriction>
3677     </xs:complexContent>
3678   </xs:complexType>
3679
3680   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3681
3682   <xs:complexType name="AuthnMethodType">
3683     <xs:complexContent>
3684       <xs:restriction base="ac:AuthnMethodBaseType">
3685         <xs:sequence>
3686           <xs:element ref="ac:PrincipalAuthenticationMechanism"
3687             minOccurs="0"/>
3688           <xs:element ref="Authenticator"/>
3689           <xs:element ref="AuthenticatorTransportProtocol"/>
3690           <xs:element ref="ac:Extension" minOccurs="0"
3691             maxOccurs="unbounded"/>
3692         </xs:sequence>
3693       </xs:restriction>
3694     </xs:complexContent>
3695   </xs:complexType>
3696
3697   <xs:element name="Authenticator" type="AuthenticatorType"/>
3698
3699   <xs:complexType name="AuthenticatorType">
3700     <xs:complexContent>
3701       <xs:restriction base="ac:AuthenticatorBaseType">
3702         <xs:sequence>
3703           <xs:element ref="ac:SubscriberLineNumber"/>
3704           <xs:element ref="ac:UserSuffix"/>
3705         </xs:sequence>

```



```

3706     </xs:restriction>
3707     </xs:complexContent>
3708   </xs:complexType>
3709
3710   <xs:element name="AuthenticatorTransportProtocol"
3711 type="TransportType"/>
3712
3713   <xs:complexType name="TransportType">
3714     <xs:complexContent>
3715       <xs:restriction base="ac:AuthenticatorTransportProtocolType">
3716         <xs:choice>
3717           <xs:element ref="ac:PSTN"/>
3718           <xs:element ref="ac:ISDN"/>
3719           <xs:element ref="ac:ADSL"/>
3720         </xs:choice>
3721       </xs:restriction>
3722     </xs:complexContent>
3723   </xs:complexType>
3724 </xs:schema>
3725

```

3726 3.4.21 Telephony (Authenticated)

3727 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony

3728 Note that this URI is also used as the target namespace in the corresponding authentication context class
3729 schema document [SAMLAC-TAuthn].

3730 Indicates that the Principal authenticated via the means of the line number, a user suffix, and a password
3731 element.

```

3732 <?xml version="1.0" encoding="UTF-8"?>
3733
3734 <xs:schema
3735 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTele
3736 phony"
3737 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3738 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3739 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3740 finalDefault="extension">
3741
3742   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3743 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3744
3745   <xs:annotation>
3746     <xs:documentation>
3747       urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
3748     </xs:documentation>
3749   </xs:annotation>
3750
3751   <xs:complexType name="AuthnContextDeclaration">
3752     <xs:complexContent>
3753       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3754         <xs:sequence>
3755           <xs:element ref="ac:Identification" minOccurs="0"/>
3756           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3757           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3758           <xs:element ref="AuthnMethod"/>
3759           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3760           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3761             maxOccurs="unbounded"/>
3762           <xs:element ref="ac:Extension" minOccurs="0"
3763             maxOccurs="unbounded"/>
3764         </xs:sequence>
3765         <xs:attribute name="ID" type="xs:ID"/>
3766       </xs:restriction>

```

```

3767     </xs:complexContent>
3768 </xs:complexType>
3769
3770 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3771
3772 <xs:complexType name="AuthnMethodType">
3773   <xs:complexContent>
3774     <xs:restriction base="ac:AuthnMethodBaseType">
3775       <xs:sequence>
3776         <xs:element ref="ac:PrincipalAuthenticationMechanism"
3777 minOccurs="0"/>
3778         <xs:element ref="Authenticator"/>
3779         <xs:element ref="AuthenticatorTransportProtocol"/>
3780         <xs:element ref="ac:Extension" minOccurs="0"
3781 maxOccurs="unbounded"/>
3782       </xs:sequence>
3783     </xs:restriction>
3784   </xs:complexContent>
3785 </xs:complexType>
3786
3787 <xs:element name="Authenticator" type="AuthenticatorType"/>
3788
3789 <xs:complexType name="AuthenticatorType">
3790   <xs:complexContent>
3791     <xs:restriction base="ac:AuthenticatorBaseType">
3792       <xs:sequence>
3793         <xs:element ref="ac:SubscriberLineNumber"/>
3794         <xs:element ref="ac:UserSuffix"/>
3795         <xs:element ref="ac:Password"/>
3796       </xs:sequence>
3797     </xs:restriction>
3798   </xs:complexContent>
3799 </xs:complexType>
3800
3801 <xs:element name="AuthenticatorTransportProtocol"
3802 type="TransportType"/>
3803
3804 <xs:complexType name="TransportType">
3805   <xs:complexContent>
3806     <xs:restriction base="ac:AuthenticatorTransportProtocolType">
3807       <xs:choice>
3808         <xs:element ref="ac:PSTN"/>
3809         <xs:element ref="ac:ISDN"/>
3810         <xs:element ref="ac:ADSL"/>
3811       </xs:choice>
3812     </xs:restriction>
3813   </xs:complexContent>
3814 </xs:complexType>
3815
3816 </xs:schema>

```

3817 3.4.22 Secure Remote Password

3818 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword

3819 Note that this URI is also used as the target namespace in the corresponding authentication context class
3820 schema document [SAMLAC-SRP]).

3821 The Secure Remote Password class is indicated when the authentication was performed by means of
3822 Secure Remote Password as specified in [RFC 2945].

```

3823 <?xml version="1.0" encoding="UTF-8"?>
3824
3825 <xs:schema
3826 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRem
3827 otePassword"

```

```

3828     xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3829     xmlns:xs="http://www.w3.org/2001/XMLSchema"
3830     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassw
3831 ord"
3832     finalDefault="extension">
3833
3834     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3835 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3836
3837     <xs:annotation>
3838         <xs:documentation>
3839             urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
3840         </xs:documentation>
3841     </xs:annotation>
3842
3843     <xs:complexType name="AuthnContextDeclaration">
3844         <xs:complexContent>
3845             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3846                 <xs:sequence>
3847                     <xs:element ref="ac:Identification" minOccurs="0"/>
3848                     <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3849                     <xs:element ref="ac:OperationalProtection"
3850 minOccurs="0"/>
3851                     <xs:element ref="AuthnMethod"/>
3852                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3853                     <xs:element ref="ac:AuthenticatingAuthority"
3854 minOccurs="0"
3855                             maxOccurs="unbounded"/>
3856                     <xs:element ref="ac:Extension" minOccurs="0"
3857                             maxOccurs="unbounded"/>
3858                 </xs:sequence>
3859                 <xs:attribute name="ID" type="xs:ID"/>
3860             </xs:restriction>
3861         </xs:complexContent>
3862     </xs:complexType>
3863
3864     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3865
3866     <xs:complexType name="AuthnMethodType">
3867         <xs:complexContent>
3868             <xs:restriction base="ac:AuthnMethodBaseType">
3869                 <xs:sequence>
3870                     <xs:element ref="PrincipalAuthenticationMechanism"/>
3871                     <xs:element ref="Authenticator"/>
3872                     <xs:element ref="ac:AuthenticatorTransportProtocol"
3873 minOccurs="0"/>
3874                     <xs:element ref="ac:Extension" minOccurs="0"
3875                             maxOccurs="unbounded"/>
3876                 </xs:sequence>
3877             </xs:restriction>
3878         </xs:complexContent>
3879     </xs:complexType>
3880
3881     <xs:element name="PrincipalAuthenticationMechanism"
3882 type="PasswordAuthnMechanismType"/>
3883
3884     <xs:complexType name="PasswordAuthnMechanismType">
3885         <xs:complexContent>
3886             <xs:restriction
3887 base="ac:PrincipalAuthenticationMechanismType">
3888                 <xs:sequence>

```

```

3889         <xs:choice>
3890             <xs:element ref="ac:RestrictedPassword"/>
3891         </xs:choice>
3892     </xs:sequence>
3893 </xs:restriction>
3894 </xs:complexContent>
3895 </xs:complexType>
3896
3897 <xs:element name="Authenticator" type="SharedSecretType"/>
3898
3899 <xs:complexType name="SharedSecretType">
3900     <xs:complexContent>
3901         <xs:restriction base="ac:AuthenticatorBaseType">
3902             <xs:choice>
3903                 <xs:element ref="SharedSecretChallengeResponse"/>
3904             </xs:choice>
3905         </xs:restriction>
3906     </xs:complexContent>
3907 </xs:complexType>
3908
3909 <xs:element name="SharedSecretChallengeResponse"
3910 type="ChallengeResponseType"/>
3911
3912 <xs:complexType name="ChallengeResponseType">
3913     <xs:complexContent>
3914         <xs:restriction base="ac:SharedSecretChallengeResponseType">
3915             <xs:attribute name="method" fixed="urn:ietf:rfc:2945"/>
3916         </xs:restriction>
3917     </xs:complexContent>
3918 </xs:complexType>
3919
3920 </xs:schema>

```

3921 **3.4.23 SSL/TLS Certificate-Based Client Authentication**

3922 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient

3923 Note that this URI is also used as the target namespace in the corresponding authentication context class
3924 schema document [SAMLAC-SSL]).

3925 This class indicates that the Principal authenticated by means of a client certificate, secured with the
3926 SSL/TLS transport.

```

3927 <?xml version="1.0" encoding="UTF-8"?>
3928
3929 <xs:schema
3930 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
3931 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3932 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3933 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
3934 finalDefault="extension">
3935
3936     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3937 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3938
3939     <xs:annotation>
3940         <xs:documentation>
3941             urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
3942         </xs:documentation>
3943     </xs:annotation>
3944

```

```

3945 <xs:complexType name="AuthnContextDeclaration">
3946 <xs:complexContent>
3947 <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3948 <xs:sequence>
3949 <xs:element ref="ac:Identification" minOccurs="0"/>
3950 <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3951 <xs:element ref="ac:OperationalProtection"
3952 minOccurs="0"/>
3953 <xs:element ref="AuthnMethod"/>
3954 <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3955 <xs:element ref="ac:AuthenticatingAuthority"
3956 minOccurs="0"
3957 maxOccurs="unbounded"/>
3958 <xs:element ref="ac:Extension" minOccurs="0"
3959 maxOccurs="unbounded"/>
3960 </xs:sequence>
3961 <xs:attribute name="ID" type="xs:ID"/>
3962 </xs:restriction>
3963 </xs:complexContent>
3964 </xs:complexType>
3965
3966 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3967
3968 <xs:complexType name="AuthnMethodType">
3969 <xs:complexContent>
3970 <xs:restriction base="ac:AuthnMethodBaseType">
3971 <xs:sequence>
3972 <xs:element ref="AuthnMechanism"/>
3973 <xs:element ref="Authenticator"/>
3974 <xs:element ref="AuthenticatorTransportProtocol"
3975 minOccurs="0"/>
3976 <xs:element ref="ac:Extension" minOccurs="0"
3977 maxOccurs="unbounded"/>
3978 </xs:sequence>
3979 </xs:restriction>
3980 </xs:complexContent>
3981 </xs:complexType>
3982
3983 <xs:element name="AuthnMechanism"
3984 type="PasswordAuthnMechanismType"/>
3985
3986 <xs:complexType name="PasswordAuthnMechanismType">
3987 <xs:complexContent>
3988 <xs:restriction
3989 base="ac:PrincipalAuthenticationMechanismType">
3990 <xs:sequence>
3991 <xs:choice>
3992 <xs:element ref="ac:RestrictedPassword"/>
3993 </xs:choice>
3994 </xs:sequence>
3995 <xs:attribute name="preauth" type="xs:integer"
3996 use="optional"/>
3997 </xs:restriction>
3998 </xs:complexContent>
3999 </xs:complexType>
4000
4001 <xs:element name="Authenticator" type="AuthenticatorType"/>
4002
4003 <xs:complexType name="AuthenticatorType">
4004 <xs:complexContent>
4005 <xs:restriction base="ac:AuthenticatorBaseType">

```

```

4006     <xs:choice>
4007         <xs:element ref="DigSig"/>
4008     </xs:choice>
4009 </xs:restriction>
4010 </xs:complexContent>
4011 </xs:complexType>
4012
4013 <xs:element name="DigSig" type="DigSigType"/>
4014
4015 <xs:complexType name="DigSigType">
4016     <xs:complexContent>
4017         <xs:restriction base="ac:PublicKeyType">
4018             <xs:attribute name="keyValidation"
4019 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
4020         </xs:restriction>
4021     </xs:complexContent>
4022 </xs:complexType>
4023
4024 <xs:element name="AuthenticatorTransportProtocol"
4025 type="ProtectedProtocolType"/>
4026
4027 <xs:complexType name="ProtectedProtocolType">
4028     <xs:complexContent>
4029         <xs:restriction
4030 base="ac:AuthenticatorTransportProtocolType">
4031             <xs:choice>
4032                 <xs:element ref="ac:SSL"/>
4033                 <xs:element ref="ac:WTLS"/>
4034             </xs:choice>
4035         </xs:restriction>
4036     </xs:complexContent>
4037 </xs:complexType>
4038
4039 </xs:schema>

```

4040 **3.4.24 TimeSyncToken**

4041 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken

4042 Note that this URI is also used as the target namespace in the corresponding authentication context class
4043 schema document [SAMLAC-TST]).

4044 The TimeSyncToken class is identified when a Principal authenticates through a time synchronization
4045 token.

```

4046 <?xml version="1.0" encoding="UTF-8"?>
4047
4048 <xs:schema
4049 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
4050 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
4051 xmlns:xs="http://www.w3.org/2001/XMLSchema"
4052 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
4053 finalDefault="extension">
4054
4055     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
4056 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
4057
4058     <xs:annotation>
4059         <xs:documentation>
4060             urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
4061         </xs:documentation>
4062     </xs:annotation>
4063

```

```

4064 <xs:complexType name="AuthnContextDeclaration">
4065   <xs:complexContent>
4066     <xs:restriction base="ac:AuthnContextDeclarationBaseType">
4067       <xs:sequence>
4068         <xs:element ref="ac:Identification" minOccurs="0"/>
4069         <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
4070         <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
4071         <xs:element ref="AuthnMethod"/>
4072         <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
4073         <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
4074           maxOccurs="unbounded"/>
4075         <xs:element ref="ac:Extension" minOccurs="0"
4076           maxOccurs="unbounded"/>
4077       </xs:sequence>
4078       <xs:attribute name="ID" type="xs:ID"/>
4079     </xs:restriction>
4080   </xs:complexContent>
4081 </xs:complexType>
4082
4083 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
4084
4085 <xs:complexType name="AuthnMethodType">
4086   <xs:complexContent>
4087     <xs:restriction base="ac:AuthnMethodBaseType">
4088       <xs:sequence>
4089         <xs:element ref="PrincipalAuthenticationMechanism"
4090 minOccurs="0"/>
4091         <xs:element ref="ac:Authenticator"/>
4092         <xs:element ref="ac:AuthenticatorTransportProtocol"
4093           minOccurs="0"/>
4094         <xs:element ref="ac:Extension" minOccurs="0"
4095           maxOccurs="unbounded"/>
4096       </xs:sequence>
4097     </xs:restriction>
4098   </xs:complexContent>
4099 </xs:complexType>
4100
4101 <xs:element name="PrincipalAuthenticationMechanism"
4102 type="TimeSyncMechType"/>
4103
4104 <xs:complexType name="TimeSyncMechType">
4105   <xs:complexContent>
4106     <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
4107       <xs:choice>
4108         <xs:element ref="Token"/>
4109       </xs:choice>
4110     </xs:restriction>
4111   </xs:complexContent>
4112 </xs:complexType>
4113
4114 <xs:element name="Token" type="TokenType"/>
4115
4116 <xs:complexType name="TokenType">
4117   <xs:complexContent>
4118     <xs:restriction base="ac:TokenType">
4119       <xs:sequence>
4120         <xs:element ref="TimeSyncToken"/>
4121         <xs:element ref="ac:Extension" minOccurs="0"
4122 maxOccurs="unbounded"/>
4123       </xs:sequence>
4124     </xs:restriction>
4125   </xs:complexContent>
4126 </xs:complexType>
4127
4128 <xs:element name="TimeSyncToken" type="TimeSyncTokenType"/>
4129
4130 <xs:complexType name="TimeSyncTokenType">

```

```
4131 <xs:complexContent>
4132 <xs:restriction base="ac:TimeSyncTokenType">
4133
4134 <xs:attribute name="DeviceType" use="required">
4135 <xs:simpleType>
4136 <xs:restriction base="xs:NMTOKEN">
4137 <xs:enumeration value="hardware"/>
4138 </xs:restriction>
4139 </xs:simpleType>
4140 </xs:attribute>
4141
4142 <xs:attribute name="SeedLength" use="required">
4143 <xs:simpleType>
4144 <xs:restriction base="xs:integer">
4145 <xs:minInclusive value="64"/>
4146 </xs:restriction>
4147 </xs:simpleType>
4148 </xs:attribute>
4149
4150 <xs:attribute name="DeviceInHand" use="required">
4151 <xs:simpleType>
4152 <xs:restriction base="xs:NMTOKEN">
4153 <xs:enumeration value="true"/>
4154 </xs:restriction>
4155 </xs:simpleType>
4156 </xs:attribute>
4157 </xs:restriction>
4158 </xs:complexContent>
4159 </xs:complexType>
4160
4161 </xs:schema>
```

4162 **3.4.25 Unspecified**

4163 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

4164 The Unspecified class indicates that the authentication was performed by unspecified means.

4 References

4165

- 4166 **[RFC 1510]** J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5)*. IETF
4167 RFC 1510, September 1993. <http://www.ietf.org/rfc/rfc1510.txt>.
- 4168 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
4169 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 4170 **[RFC 2945]** T. Wu. *The SRP Authentication and Key Exchange System*. IETF RFC 2945,
4171 September 2000. <http://www.ietf.org/rfc/rfc2945.txt>.
- 4172 **[SAMLAC-xsd]** J. Kemp et al., SAML authentication context schema. OASIS SSTC, August
4173 2004. Document ID sstc-saml-schema-authn-context-1.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
4174 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 4175 **[SAMLAC-IP]** J. Kemp et al., SAML context class schema for Internet Protocol. OASIS SSTC,
4176 August 2004. Document ID sstc-saml-schema-authn-context-ip-1.0. See
4177 <http://www.oasis-open.org/committees/security/>.
- 4178 **[SAMLAC-IPP]** J. Kemp et al., SAML context class schema for Internet Protocol Password.
4179 OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-
4180 ippword-1.0. See <http://www.oasis-open.org/committees/security/>.
- 4181 **[SAMLAC-Kerb]** J. Kemp et al., SAML context class schema for Kerberos. OASIS SSTC, August
4182 2004. Document ID sstc-saml-schema-authn-context-kerberos-1.0. See
4183 <http://www.oasis-open.org/committees/security/>.
- 4184 **[SAMLAC-MOFC]** J. Kemp et al., SAML context class schema for Mobile One Factor Contract.
4185 Document ID sstc-saml-schema-authn-context-mobileonefactor-reg-1.0. See
4186 OASIS SSTC, August 2004. <http://www.oasis-open.org/committees/security/>.
- 4187 **[SAMLAC-MOFU]** J. Kemp et al., SAML context class schema for Mobile One Factor Unregistered.
4188 Document ID sstc-saml-schema-authn-context-mobileonefactor-unreg-1.0. See
4189 OASIS SSTC, August 2004. <http://www.oasis-open.org/committees/security/>.
- 4190 **[SAMLAC-MTFC]** J. Kemp et al., SAML context class schema for Mobile Two Factor Contract.
4191 OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-
4192 mobiletwofactor-reg-1.0. See <http://www.oasis-open.org/committees/security/>.
- 4193 **[SAMLAC-MTFU]** J. Kemp et al., SAML context class schema for Mobile Two Factor Unregistered.
4194 OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-
4195 mobiletwofactor-unreg-1.0. See <http://www.oasis-open.org/committees/security/>.
- 4196 **[SAMLAC-Pass]** J. Kemp et al., SAML context class schema for Password. OASIS SSTC, August
4197 2004. Document ID sstc-saml-schema-authn-context-pword-1.0. See
4198 <http://www.oasis-open.org/committees/security/>.
- 4199 **[SAMLAC-PGP]** J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC,
4200 August 2004. Document ID sstc-saml-schema-authn-context-pgp-1.0. See
4201 <http://www.oasis-open.org/committees/security/>.
- 4202 **[SAMLAC-PPT]** J. Kemp et al., SAML context class schema for Password Protected Transport.
4203 OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-ppt-
4204 1.0. See <http://www.oasis-open.org/committees/security/>.
- 4205 **[SAMLAC-Prev]** J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC,
4206 August 2004. Document ID sstc-saml-schema-authn-context-session-1.0. See
4207 <http://www.oasis-open.org/committees/security/>.
- 4208 **[SAMLAC-Smart]** J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC, August
4209 2004. Document ID sstc-saml-schema-authn-context-smartcard-1.0. See
4210 <http://www.oasis-open.org/committees/security/>.
- 4211 **[SAMLAC-SmPKI]** J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC,
4212 August 2004. Document ID sstc-saml-schema-authn-context-smartcardpki-1.0.

4213		See http://www.oasis-open.org/committees/security/ .
4214	[SAMLAC-SPKI]	J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-spki-1.0. See http://www.oasis-open.org/committees/security/ .
4215		
4216		
4217	[SAMLAC-SRP]	J. Kemp et al., SAML context class schema for Secure Remote Password. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-srp-1.0. See http://www.oasis-open.org/committees/security/ .
4218		
4219		
4220	[SAMLAC-SSL]	J. Kemp et al., SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-sslcert-1.0. See http://www.oasis-open.org/committees/security/ .
4221		
4222		
4223	[SAMLAC-SwPKI]	J. Kemp et al., SAML context class schema for Software PKI. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-softwarepki-1.0. See http://www.oasis-open.org/committees/security/ .
4224		
4225		
4226	[SAMLAC-Tele]	J. Kemp et al., SAML context class schema for Telephony. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-telephony-1.0. See http://www.oasis-open.org/committees/security/ .
4227		
4228		
4229	[SAMLAC-TNom]	J. Kemp et al., SAML context class schema for Telephony (“Nomadic”). OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-nomad-telephony-1.0. See http://www.oasis-open.org/committees/security/ .
4230		
4231		
4232	[SAMLAC-TPers]	J. Kemp et al., SAML context class schema for Telephony (Personalized). OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-personal-telephony-1.0. See http://www.oasis-open.org/committees/security/ .
4233		
4234		
4235	[SAMLAC-TAuthn]	J. Kemp et al., SAML context class schema for Telephony (Authenticated). OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-auth-telephony-1.0. See http://www.oasis-open.org/committees/security/ .
4236		
4237		
4238	[SAMLAC-TST]	J. Kemp et al., SAML context class schema for Time Sync Token. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-timesync-1.0. See http://www.oasis-open.org/committees/security/ .
4239		
4240		
4241	[SAMLAC-X509]	J. Kemp et al., SAML context class schema for Public Key – X.509. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-x509-1.0. See http://www.oasis-open.org/committees/security/ .
4242		
4243		
4244	[SAMLAC-XSig]	J. Kemp et al., SAML context class schema for Public Key – XML Signature. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-xmldsig-1.0. See http://www.oasis-open.org/committees/security/ .
4245		
4246		
4247	[SAMLCore]	S. Cantor et al., <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, August 2004. Document ID sstc-saml-core-2.0-cd-01. See http://www.oasis-open.org/committees/security/ .
4248		
4249		
4250	[Schema1]	H. S. Thompson et al. <i>XML Schema Part 1: Structures</i> . World Wide Web Consortium Recommendation, May 2001. http://www.w3.org/TR/xmlschema-1/ .
4251		
4252	[XMLSig]	D. Eastlake et al., <i>XML-Signature Syntax and Processing</i> , World Wide Web Consortium, February 2002. http://www.w3.org/TR/xmldsig-core/ .
4253		

4254 **Appendix A. Acknowledgments**

4255 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
4256 Committee, whose voting members at the time of publication were:

- 4257 • Conor Cahill, AOL
- 4258 • Hal Lockhart, BEA Systems
- 4259 • Rick Randall, Booz Allen Hamilton
- 4260 • Ronald Jacobson, Computer Associates
- 4261 • Gavenraj Sodhi, Computer Associates
- 4262 • Tim Alsop, CyberSafe Limited
- 4263 • Paul Madsen, Entrust
- 4264 • Carolina Canales-Valenzuela, Ericsson
- 4265 • Dana Kaufman, Forum Systems
- 4266 • Irving Reid, Hewlett-Packard
- 4267 • Paula Austel, IBM
- 4268 • Maryann Hondo, IBM
- 4269 • Michael McIntosh, IBM
- 4270 • Anthony Nadalin, IBM
- 4271 • Nick Ragouzis, Individual
- 4272 • Scott Cantor, Internet2
- 4273 • Bob Morgan, Internet2
- 4274 • Prateek Mishra, Netegrity
- 4275 • Forest Yin, Netegrity
- 4276 • Peter Davis, Neustar
- 4277 • Frederick Hirsch, Nokia
- 4278 • John Kemp, Nokia
- 4279 • Senthil Sengodan, Nokia
- 4280 • Scott Kiestler, Novell
- 4281 • Steve Anderson, OpenNetwork
- 4282 • Ari Kermaier, Oracle
- 4283 • Vamsi Motukuru, Oracle
- 4284 • Darren Platt, Ping Identity
- 4285 • Jim Lien, RSA Security
- 4286 • John Linn, RSA Security
- 4287 • Rob Philpott, RSA Security
- 4288 • Dipak Chopra, SAP
- 4289 • Jahan Moreh, Sigaba
- 4290 • Bhavna Bhatnagar, Sun Microsystems
- 4291 • Jeff Hodges, Sun Microsystems
- 4292 • Eve Maler, Sun Microsystems
- 4293 • Ronald Monzillo, Sun Microsystems
- 4294 • Emily Xu, Sun Microsystems
- 4295 • Mike Beach, Boeing

4296 • Greg Whitehead, Trustgenix

4297 • James Vanderbeek, Vodafone

4298

4299 The editors also would like to acknowledge the following people for their contributions to previous versions
4300 of the OASIS Security Assertions Markup Language Standard:

4301 • Stephen Farrell, Baltimore Technologies

4302 • David Orchard, BEA Systems

4303 • Krishna Sankar, Cisco Systems

4304 • Zahid Ahmed, CommerceOne

4305 • Carlisle Adams, Entrust

4306 • Tim Moses, Entrust

4307 • Nigel Edwards, Hewlett-Packard

4308 • Joe Pato, Hewlett-Packard

4309 • Bob Blakley, IBM

4310 • Marlena Erdos, IBM

4311 • Marc Chanliau, Netegrity

4312 • Chris McLaren, Netegrity

4313 • Lynne Rosenthal, NIST

4314 • Mark Skall, NIST

4315 • Simon Godik, Overxeer

4316 • Charles Norwood, SAIC

4317 • Evan Prodromou, Securant

4318 • Robert Griffin, RSA Security (former editor)

4319 • Sai Allarvarpu, Sun Microsystems

4320 • Chris Ferris, Sun Microsystems

4321 • Emily Xu, Sun Microsystems

4322 • Mike Myers, Traceroute Security

4323 • Phillip Hallam-Baker, VeriSign (former editor)

4324 • James Vanderbeek, Vodafone

4325 • Mark O'Neill, Vordel

4326 • Tony Palmer, Vordel

4327

4328 Finally, the editors wish to acknowledge the following people for their contributions of material used as
4329 input to the OASIS Security Assertions Markup Language specifications:

4330 • Thomas Gross, IBM

4331 • Birgit Pfitzmann, IBM

4332 Appendix B. Notices

4333 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
4334 might be claimed to pertain to the implementation or use of the technology described in this document or
4335 the extent to which any license under such rights might or might not be available; neither does it represent
4336 that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to
4337 rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made
4338 available for publication and any assurances of licenses to be made available, or the result of an attempt
4339 made to obtain a general license or permission for the use of such proprietary rights by implementors or
4340 users of this specification, can be obtained from the OASIS Executive Director.

4341 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or
4342 other proprietary rights which may cover technology that may be required to implement this specification.
4343 Please address the information to the OASIS Executive Director.

4344 **Copyright © OASIS Open 2004. All Rights Reserved.**

4345 This document and translations of it may be copied and furnished to others, and derivative works that
4346 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and
4347 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
4348 this paragraph are included on all such copies and derivative works. However, this document itself does
4349 not be modified in any way, such as by removing the copyright notice or references to OASIS, except as
4350 needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights
4351 defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it
4352 into languages other than English.

4353 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
4354 or assigns.

4355 This document and the information contained herein is provided on an "AS IS" basis and OASIS
4356 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
4357 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR
4358 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.