



1

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

5 **Last-Call Working Draft 07, 13 July 2004**

6 **Document identifier:**

7 sstc-saml-authn-context-2.0-draft-07

8 **Location:**

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

10 **Editors:**

11 John Kemp, Nokia
12 Eve Maler, Sun Microsystems

13 **Contributors:**

14 Paul Madsen, Entrust

15 **Abstract:**

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

18 **Status:**

19 This is a last-call working draft produced by the Security Services Technical Committee. **See the**
20 **Revision History for details of changes made in this revision.**

21 Comments on this last-call draft are solicited by **2 August 2004** so that the TC can subsequently
22 prepare an OASIS Committee Draft. Committee members should submit comments and potential
23 errata to the security-services@lists.oasis-open.org list. Others should submit them by filling in the
24 form at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The
25 committee will publish vetted errata on the Security Services TC web page ([http://www.oasis-](http://www.oasis-open.org/committees/security/)
26 [open.org/committees/security/](http://www.oasis-open.org/committees/security/)).

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

31 Table of Contents

32	1 Introduction.....	3
33	1.1 Authentication Context Concepts.....	3
34	1.2 Notation and Terminology.....	3
35	1.2.1 Notational Conventions.....	3
36	1.2.2 Namespaces.....	4
37	2 Authentication Context Declaration.....	5
38	2.1 Data Model.....	5
39	2.2 Extensibility.....	6
40	2.3 Processing Rules.....	6
41	2.4 Schema.....	6
42	3 Authentication Context Classes.....	23
43	3.1 Advantages of Authentication Context Classes.....	23
44	3.2 Processing Rules.....	23
45	3.3 Extensibility.....	24
46	3.4 Schemas.....	24
47	3.4.1 Internet Protocol.....	24
48	3.4.2 InternetProtocolPassword.....	26
49	3.4.3 Kerberos.....	27
50	3.4.4 MobileOneFactorUnregistered.....	29
51	3.4.5 MobileTwoFactorUnregistered.....	32
52	3.4.6 MobileOneFactorContract.....	35
53	3.4.7 MobileTwoFactorContract.....	39
54	3.4.8 Password.....	42
55	3.4.9 PasswordProtectedTransport.....	44
56	3.4.10 PreviousSession.....	45
57	3.4.11 Public Key – X.509.....	46
58	3.4.12 Public Key – PGP.....	48
59	3.4.13 Public Key – SPKI.....	50
60	3.4.14 Public Key - XML Digital Signature.....	52
61	3.4.15 Smartcard.....	53
62	3.4.16 SmartcardPKI.....	54
63	3.4.17 SoftwarePKI.....	57
64	3.4.18 Telephony.....	59
65	3.4.19 Telephony ("Nomadic").....	60
66	3.4.20 Telephony (Personalized).....	62
67	3.4.21 Telephony (Authenticated).....	63
68	3.4.22 Secure Remote Password.....	65
69	3.4.23 SSL/TLS Certificate-Based Client Authentication.....	66
70	3.4.24 TimeSyncToken.....	68
71	3.4.25 Unspecified.....	70
72	4 References.....	71
73	5 Acknowledgments.....	72
74	6 Revision History.....	73
75	7 Notices.....	74
76		

77 1 Introduction

78 This specification defines a syntax for the definition of authentication context declarations and an initial list
79 of OASIS SSTC authentication context classes.

80 1.1 Authentication Context Concepts

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

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

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

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

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

109 1.2 Notation and Terminology

110 This section specifies the notations, namespaces and and terminology used throughout this specification.
111 This specification uses schema documents conforming to W3C XML Schema [XMLSchema] and
112 normative text to describe the syntax and semantics of XML-encoded messages.

113 1.2.1 Notational Conventions

114 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
115 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described
116 in RFC 2119.

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

120 Listings of XML schemas appear like this.

121 1.2.2 Namespaces

122 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
123 their respective namespaces as follows, whether or not a namespace declaration is present in the
124 example:

Prefix	XML Namespace	Comments
ac:	urn:oasis:names:tc:SAML:2.0:ac	This is the namespace defined in this specification.
xsi:	http://www.w3.org/2001/XMLSchema	
xsi:	http://www.w3.org/2001/XMLSchema-instance	

125

126 This specification uses the following typographical conventions in text: <AuthnContextElement>,
127 <ns:ForeignElement>, XMLAttribute, **Datatype**, OtherKeyword.

2 Authentication Context Declaration

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

- 132 • What were the initial user identification mechanisms (for example, face-to-face, online, shared
133 secret).
- 134 • What are the mechanisms for minimizing compromise of credentials (for example, credential
135 renewal frequency, client-side key generation).
- 136 • What are the mechanisms for storing and protecting credentials (for example, smartcard, password
137 rules).
- 138 • What was the authentication mechanism or method (for example, password, certificate-based SSL).

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

142 A SAML authentication authority will deliver to a relying party the additional authentication context
143 information in the form of an Authentication Context Declaration, an XML document either inserted directly
144 or referenced within the `<AuthnResponse>` message that the authentication authority returns to the
145 relying party.

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

2.1 Data Model

152 A particular SSTC authentication context declaration will capture the characteristics of the processes,
153 procedures, and mechanisms by which the authentication verified the subject before issuing an identity,
154 protects the secrets on which subsequent authentications are based, and the mechanisms used for this
155 authentication. These characteristics are categorized in the Authentication Context schema as follows:

- 156 • Identification - Characteristics that describe the processes and mechanism the authentication
157 authority uses to initially create an association between a subject and the identity (or name) by which
158 the subject will be known.
- 159 • Technical Protection - Characteristics that describe how the "secret" (the knowledge or possession
160 of which allows the subject to authenticate to the authentication authority) is kept secure.
- 161 • Operational Protection - Characteristics that describe procedural security controls employed by the
162 authentication authority (for example, security audits, records archival).
- 163 • Authentication Method - Characteristics that define the mechanisms by which the subject of the
164 issued assertion authenticates to the authentication authority (for example, a password versus a
165 smartcard).
- 166 • Governing Agreements - Characteristics that describe the legal framework (e.g. liability constraints
167 and contractual obligations) underlying the authentication event and/or its associated technical
168 authentication infrastructure.

169 2.2 Extensibility

170 The Authentication Context Declaration schema has well-defined extensibility points through the
171 <Extension> element. Authentication authorities can use this element to insert additional authentication
172 context details for the SAML assertions they issue (assuming that the consuming relying party will be able
173 to understand these extensions). These additional elements MUST be in a separate XML Namespace to
174 that of the base Authentication Context Declaration schema.

175 2.3 Processing Rules

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

178 2.4 Schema

179 This section lists the complete Authentication Context XML Schema.

```
180 <?xml version="1.0" encoding="UTF-8"?>
181 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
182   xmlns:xs="http://www.w3.org/2001/XMLSchema"
183   xmlns="urn:oasis:names:tc:SAML:2.0:ac">
184
185   <xs:element name="AuthenticationContextDeclaration"
186     type="AuthnContextDeclarationBaseType">
187     <xs:annotation>
188       <xs:documentation>
189         A particular assertion on an identity
190         provider's part with respect to the authentication
191         context associated with an authentication assertion.
192       </xs:documentation>
193     </xs:annotation>
194   </xs:element>
195
196   <xs:element name="Identification" type="IdentificationType">
197     <xs:annotation>
198       <xs:documentation>
199         Refers to those characteristics that describe the
200         processes and mechanisms
201         the Authentication Authority uses to initially create
202         an association between a Principal
203         and the identity (or name) by which the Principal will
204         be known
205       </xs:documentation>
206     </xs:annotation>
207   </xs:element>
208
209   <xs:element name="PhysicalVerification">
210     <xs:annotation>
211       <xs:documentation>
212         This element indicates that identification has been
213         performed in a physical
214         face-to-face meeting with the principal and not in an
215         online manner.
216       </xs:documentation>
217     </xs:annotation>
218     <xs:complexType>
219       <xs:attribute name="credentialLevel">
220         <xs:simpleType>
221           <xs:restriction base="xs:NMTOKEN">
```

```

222         <xs:enumeration value="primary"/>
223         <xs:enumeration value="secondary"/>
224     </xs:restriction>
225 </xs:simpleType>
226 </xs:attribute>
227 </xs:complexType>
228 </xs:element>
229
230 <xs:element name="WrittenConsent">
231     <xs:complexType>
232         <xs:sequence>
233             <xs:element ref="Extension" minOccurs="0"
234                 maxOccurs="unbounded"/>
235         </xs:sequence>
236     </xs:complexType>
237 </xs:element>
238
239 <xs:element name="TechnicalProtection"
240     type="TechnicalProtectionBaseType">
241     <xs:annotation>
242         <xs:documentation>
243             Refers to those characteristics that describe how the
244             'secret' (the knowledge or possession
245             of which allows the Principal to authenticate to the
246             Authentication Authority) is kept secure
247         </xs:documentation>
248     </xs:annotation>
249 </xs:element>
250
251 <xs:element name="SecretKeyProtection"
252     type="SecretKeyProtectionType">
253     <xs:annotation>
254         <xs:documentation>
255             This element indicates the types and strengths of
256             facilities
257             of a UA used to protect a shared secret key from
258             unauthorized access and/or use.
259         </xs:documentation>
260     </xs:annotation>
261 </xs:element>
262
263 <xs:element name="PrivateKeyProtection"
264     type="PrivateKeyProtectionType">
265     <xs:annotation>
266         <xs:documentation>
267             This element indicates the types and strengths of
268             facilities
269             of a UA used to protect a private key from
270             unauthorized access and/or use.
271         </xs:documentation>
272     </xs:annotation>
273 </xs:element>
274
275 <xs:element name="KeyActivation" type="KeyActivationType">
276     <xs:annotation>
277         <xs:documentation>The actions that must be performed
278             before the private key can be used. </xs:documentation>
279     </xs:annotation>
280 </xs:element>
281
282 <xs:element name="KeySharing" type="KeySharingType">

```

```

283     <xs:annotation>
284         <xs:documentation>Whether or not the private key is shared
285             with the certificate authority.</xs:documentation>
286     </xs:annotation>
287 </xs:element>
288
289 <xs:element name="KeyStorage" type="KeyStorageType">
290     <xs:annotation>
291         <xs:documentation>
292             In which medium is the key stored.
293             memory - the key is stored in memory.
294             smartcard - the key is stored in a smartcard.
295             token - the key is stored in a hardware token.
296             MobileDevice - the key is stored in a mobile device.
297             MobileAuthCard - the key is stored in a mobile
298             authentication card.
299         </xs:documentation>
300     </xs:annotation>
301 </xs:element>
302
303 <xs:element name="SubscriberLineNumber">
304     <xs:complexType>
305         <xs:sequence>
306             <xs:element ref="Extension" minOccurs="0"
307                 maxOccurs="unbounded"/>
308         </xs:sequence>
309     </xs:complexType>
310 </xs:element>
311
312 <xs:element name="UserSuffix">
313     <xs:complexType>
314         <xs:sequence>
315             <xs:element ref="Extension" minOccurs="0"
316                 maxOccurs="unbounded"/>
317         </xs:sequence>
318     </xs:complexType>
319 </xs:element>
320
321 <xs:element name="Password" type="PasswordType">
322     <xs:annotation>
323         <xs:documentation>
324             This element indicates that a password (or passphrase)
325             has been used to
326             authenticate the Principal to a remote system.
327         </xs:documentation>
328     </xs:annotation>
329 </xs:element>
330
331 <xs:element name="ActivationPin" type="ActivationPinType">
332     <xs:annotation>
333         <xs:documentation>
334             This element indicates that a Pin (Personal
335             Identification Number) has been used to authenticate the
336             Principal to
337             some local system in order to activate a key.
338         </xs:documentation>
339     </xs:annotation>
340 </xs:element>
341
342 <xs:element name="Token" type="TokenType">
343     <xs:annotation>

```

```

344     <xs:documentation>
345         This element indicates that a hardware or software
346         token is used
347         as a method of identifying the Principal.
348     </xs:documentation>
349 </xs:annotation>
350 </xs:element>
351
352 <xs:element name="TimeSyncToken" type="TimeSyncTokenType">
353     <xs:annotation>
354         <xs:documentation>
355             This element indicates that a time synchronization
356             token is used to identify the Principal. hardware -
357             the time synchronization
358             token has been implemented in hardware. software - the
359             time synchronization
360             token has been implemented in software. SeedLength -
361             the length, in bits, of the
362             random seed used in the time synchronization token.
363         </xs:documentation>
364     </xs:annotation>
365 </xs:element>
366
367 <xs:element name="Smartcard">
368     <xs:annotation>
369         <xs:documentation>
370             This element indicates that a smartcard is used to
371             identity the Principal.
372         </xs:documentation>
373     </xs:annotation>
374     <xs:complexType>
375         <xs:sequence>
376             <xs:element ref="Extension" minOccurs="0"
377                 maxOccurs="unbounded"/>
378         </xs:sequence>
379     </xs:complexType>
380 </xs:element>
381
382 <xs:element name="Length" type="LengthType">
383     <xs:annotation>
384         <xs:documentation>
385             This element indicates the minimum and/or maximum
386             ASCII length of the password which is enforced (by the UA
387 or the
388 IdP). In other words, this is the minimum and/or maximum
389 number of
390 ASCII characters required to represent a valid password.
391 min - the minimum number of ASCII characters required
392 in a valid password, as enforced by the UA or the IdP.
393 max - the maximum number of ASCII characters required
394 in a valid password, as enforced by the UA or the IdP.
395         </xs:documentation>
396     </xs:annotation>
397 </xs:element>
398
399 <xs:element name="ActivationLimit" type="ActivationLimitType">
400     <xs:annotation>
401         <xs:documentation>
402             This element indicates the length of time for which an
403             PIN-based authentication is valid.
404         </xs:documentation>

```

```

405     </xs:annotation>
406 </xs:element>
407
408 <xs:element name="Generation">
409   <xs:annotation>
410     <xs:documentation>
411       Indicates whether the password was chosen by the
412       Principal or auto-supplied by the Authentication
413 Authority.
414       principalchosen - the Principal is allowed to choose
415       the value of the password. This is true even if
416       the initial password is chosen at random by the UA or
417       the IdP and the Principal is then free to change
418       the password.
419       automatic - the password is chosen by the UA or the
420       IdP to be cryptographically strong in some sense,
421       or to satisfy certain password rules, and that the
422       Principal is not free to change it or to choose a new
423 password.
424     </xs:documentation>
425   </xs:annotation>
426
427   <xs:complexType>
428     <xs:attribute name="mechanism" use="required">
429       <xs:simpleType>
430         <xs:restriction base="xs:NMTOKEN">
431           <xs:enumeration value="principalchosen"/>
432           <xs:enumeration value="automatic"/>
433         </xs:restriction>
434       </xs:simpleType>
435     </xs:attribute>
436   </xs:complexType>
437 </xs:element>
438
439 <xs:element name="AuthenticationMethod"
440   type="AuthnMethodBaseType">
441   <xs:annotation>
442     <xs:documentation>
443       Refers to those characteristics that define the
444       mechanisms by which the Principal authenticates to the
445 Authentication
446 Authority.
447     </xs:documentation>
448   </xs:annotation>
449 </xs:element>
450
451 <xs:element name="PrincipalAuthenticationMechanism"
452   type="PrincipalAuthenticationMechanismType">
453   <xs:annotation>
454     <xs:documentation>
455       The method that a Principal employs to perform
456       authentication to local system components.
457     </xs:documentation>
458   </xs:annotation>
459 </xs:element>
460
461 <xs:element name="Authenticator" type="AuthenticatorBaseType">
462   <xs:annotation>
463     <xs:documentation>
464       The method applied to validate a principal's
465       authentication across a network

```

```

466     </xs:documentation>
467     </xs:annotation>
468   </xs:element>
469
470   <xs:element name="PreviousSession">
471     <xs:annotation>
472       <xs:documentation>
473         Indicates that the Principal has been strongly
474         authenticated in a previous session during which the IdP
475         has set a
476         cookie in the UA. During the present session the
477         Principal has only
478         been authenticated by the UA returning the cookie to the
479         IdP.
480       </xs:documentation>
481     </xs:annotation>
482     <xs:complexType>
483       <xs:sequence>
484         <xs:element ref="Extension" minOccurs="0"
485           maxOccurs="unbounded"/>
486       </xs:sequence>
487     </xs:complexType>
488   </xs:element>
489
490   <xs:element name="ResumeSession">
491     <xs:annotation>
492       <xs:documentation>
493         Rather like PreviousSession but using stronger
494         security. A secret that was established in a previous
495         session with
496         the Authentication Authority has been cached by the local
497         system and
498         is now re-used (e.g. a Master Secret is used to derive
499         new session
500         keys in TLS, SSL, WTLS).
501       </xs:documentation>
502     </xs:annotation>
503     <xs:complexType>
504       <xs:sequence>
505         <xs:element ref="Extension" minOccurs="0"
506           maxOccurs="unbounded"/>
507       </xs:sequence>
508     </xs:complexType>
509   </xs:element>
510
511   <xs:element name="ZeroKnowledge">
512     <xs:annotation>
513       <xs:documentation>
514         This element indicates that the Principal has been
515         authenticated by a zero knowledge technique as specified
516         in ISO/IEC
517         9798-5.
518       </xs:documentation>
519     </xs:annotation>
520     <xs:complexType>
521       <xs:sequence>
522         <xs:element ref="Extension" minOccurs="0"
523           maxOccurs="unbounded"/>
524       </xs:sequence>
525     </xs:complexType>
526   </xs:element>

```

```

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

```

```

588         maxOccurs="unbounded"/>
589     </xs:sequence>
590     <xs:attribute name="keyValidation" use="optional"/>
591 </xs:complexType>
592
593 <xs:element name="IPAddress">
594     <xs:annotation>
595         <xs:documentation>
596             This element indicates that the Principal has been
597             authenticated through connection from a particular IP
598 address.
599         </xs:documentation>
600     </xs:annotation>
601     <xs:complexType>
602         <xs:sequence>
603             <xs:element ref="Extension" minOccurs="0"
604                 maxOccurs="unbounded"/>
605         </xs:sequence>
606     </xs:complexType>
607 </xs:element>
608
609 <xs:element name="SharedSecretDynamicPlaintext"
610 type="SharedSecretDynamicPlaintextType"/>
611
612 <xs:annotation>
613     <xs:documentation>
614         The local system and Authentication Authority
615         share a secret key. The local system uses this to encrypt a
616         randomised string to pass to the Authentication Authority.
617     </xs:documentation>
618 </xs:annotation>
619
620 <xs:complexType name="SharedSecretDynamicPlaintextType">
621     <xs:sequence>
622         <xs:element ref="Extension" minOccurs="0"
623             maxOccurs="unbounded"/>
624     </xs:sequence>
625 </xs:complexType>
626
627 <xs:element name="AuthenticatorTransportProtocol"
628 type="AuthenticatorTransportProtocolType">
629     <xs:annotation>
630         <xs:documentation>
631             The protocol across which Authenticator information is
632             transferred to an Authentication Authority verifier.
633         </xs:documentation>
634     </xs:annotation>
635 </xs:element>
636
637 <xs:element name="HTTP">
638     <xs:annotation>
639         <xs:documentation>
640             This element indicates that the Authenticator has been
641             transmitted using bare HTTP utilizing no additional
642 security
643             protocols.
644         </xs:documentation>
645     </xs:annotation>
646     <xs:complexType>
647         <xs:sequence>
648             <xs:element ref="Extension" minOccurs="0"

```

```

649         maxOccurs="unbounded"/>
650     </xs:sequence>
651 </xs:complexType>
652 </xs:element>
653
654 <xs:element name="IPSec">
655     <xs:annotation>
656         <xs:documentation>
657             This element indicates that the Authenticator has been
658             transmitted using a transport mechanism protected by an
659 IPSEC session.
660         </xs:documentation>
661     </xs:annotation>
662     <xs:complexType>
663         <xs:sequence>
664             <xs:element ref="Extension" minOccurs="0"
665                 maxOccurs="unbounded"/>
666         </xs:sequence>
667     </xs:complexType>
668 </xs:element>
669 <xs:element name="WTLS">
670     <xs:annotation>
671         <xs:documentation>
672             This element indicates that the Authenticator has been
673             transmitted using a transport mechanism protected by a
674 WTLS session.
675         </xs:documentation>
676     </xs:annotation>
677     <xs:complexType>
678         <xs:sequence>
679             <xs:element ref="Extension" minOccurs="0"
680                 maxOccurs="unbounded"/>
681         </xs:sequence>
682     </xs:complexType>
683 </xs:element>
684 <xs:element name="MobileNetworkNoEncryption">
685     <xs:annotation>
686         <xs:documentation>
687             This element indicates that the Authenticator has been
688             transmitted solely across a mobile network using no
689 additional
690             security mechanism.
691         </xs:documentation>
692     </xs:annotation>
693     <xs:complexType>
694         <xs:sequence>
695             <xs:element ref="Extension" minOccurs="0"
696                 maxOccurs="unbounded"/>
697         </xs:sequence>
698     </xs:complexType>
699 </xs:element>
700 <xs:element name="MobileNetworkRadioEncryption">
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="MobileNetworkEndToEndEncryption">
709     <xs:complexType>

```

```

710     <xs:sequence>
711         <xs:element ref="Extension" minOccurs="0"
712             maxOccurs="unbounded"/>
713     </xs:sequence>
714 </xs:complexType>
715 </xs:element>
716
717 <xs:element name="SSL">
718     <xs:annotation>
719         <xs:documentation>
720             This element indicates that the Authenticator has been
721             transmitted using a transport mechanism protected by an
722 SSL or TLS
723             session.
724         </xs:documentation>
725     </xs:annotation>
726     <xs:complexType>
727         <xs:sequence>
728             <xs:element ref="Extension" minOccurs="0"
729                 maxOccurs="unbounded"/>
730         </xs:sequence>
731     </xs:complexType>
732 </xs:element>
733
734 <xs:element name="PSTN">
735     <xs:complexType>
736         <xs:sequence>
737             <xs:element ref="Extension" minOccurs="0"
738                 maxOccurs="unbounded"/>
739         </xs:sequence>
740     </xs:complexType>
741 </xs:element>
742
743 <xs:element name="ISDN">
744     <xs:complexType>
745         <xs:sequence>
746             <xs:element ref="Extension" minOccurs="0"
747                 maxOccurs="unbounded"/>
748         </xs:sequence>
749     </xs:complexType>
750 </xs:element>
751
752 <xs:element name="ADSL">
753     <xs:complexType>
754         <xs:sequence>
755             <xs:element ref="Extension" minOccurs="0"
756                 maxOccurs="unbounded"/>
757         </xs:sequence>
758     </xs:complexType>
759 </xs:element>
760
761 <xs:element name="OperationalProtection"
762     type="OperationalProtectionType">
763     <xs:annotation>
764         <xs:documentation>
765             Refers to those characteristics that describe
766             procedural security controls employed by the
767 Authentication Authority.
768         </xs:documentation>
769     </xs:annotation>
770 </xs:element>

```

```

771
772     <xs:element name="SecurityAudit" type="SecurityAuditType"/>
773
774     <xs:element name="SwitchAudit">
775         <xs:complexType>
776             <xs:sequence>
777                 <xs:element ref="Extension" minOccurs="0"
778                     maxOccurs="unbounded"/>
779             </xs:sequence>
780         </xs:complexType>
781     </xs:element>
782
783     <xs:element name="DeactivationCallCenter">
784         <xs:complexType>
785             <xs:sequence>
786                 <xs:element ref="Extension" minOccurs="0"
787                     maxOccurs="unbounded"/>
788             </xs:sequence>
789         </xs:complexType>
790     </xs:element>
791
792     <xs:element name="GoverningAgreements"
793         type="GoverningAgreementsType">
794         <xs:annotation>
795             <xs:documentation>
796                 Provides a mechanism for linking to external (likely
797                 human readable) documents in which additional business
798 agreements,
799                 (e.g. liability constraints, obligations, etc) can be
800 placed.
801             </xs:documentation>
802         </xs:annotation>
803     </xs:element>
804
805     <xs:element name="GoverningAgreementRef"
806         type="GoverningAgreementRefType"/>
807
808     <xs:element name="AuthenticatingAuthority"
809         type="AuthenticatingAuthorityType">
810         <xs:annotation>
811             <xs:documentation>
812                 The Authority that originally authenticated the
813                 Principal.
814             </xs:documentation>
815         </xs:annotation>
816     </xs:element>
817
818     <xs:complexType name="IdentificationType">
819         <xs:sequence>
820             <xs:element ref="PhysicalVerification" minOccurs="0"/>
821             <xs:element ref="WrittenConsent" minOccurs="0"/>
822             <xs:element ref="Extension" minOccurs="0"
823                 maxOccurs="unbounded"/>
824         </xs:sequence>
825         <xs:attribute name="nym">
826             <xs:annotation>
827                 <xs:documentation>
828                     This attribute indicates whether or not the
829                     Identification mechanisms allow the actions of the
830 Principal to be
831                     linked to an actual end user.

```

```

832     </xs:documentation>
833     </xs:annotation>
834     <xs:simpleType>
835         <xs:restriction base="xs:NMTOKEN">
836             <xs:enumeration value="anonymity"/>
837             <xs:enumeration value="verinymity"/>
838             <xs:enumeration value="pseudonymity"/>
839         </xs:restriction>
840     </xs:simpleType>
841 </xs:attribute>
842 </xs:complexType>
843
844 <xs:complexType name="GoverningAgreementsType">
845     <xs:sequence>
846         <xs:element ref="GoverningAgreementRef"
847             maxOccurs="unbounded"/>
848     </xs:sequence>
849 </xs:complexType>
850
851 <xs:complexType name="GoverningAgreementRefType">
852     <xs:attribute name="governingAgreementRef" type="xs:anyURI"
853         use="required"/>
854 </xs:complexType>
855
856 <xs:complexType name="AuthenticatingAuthorityType">
857     <xs:sequence>
858         <xs:element ref="GoverningAgreements"/>
859     </xs:sequence>
860     <xs:attribute name="ID" type="xs:anyURI" use="required"/>
861 </xs:complexType>
862
863 <xs:complexType name="AuthenticatorTransportProtocolType">
864     <xs:choice>
865         <xs:element ref="HTTP"/>
866         <xs:element ref="SSL"/>
867         <xs:element ref="MobileNetworkNoEncryption"/>
868         <xs:element ref="MobileNetworkRadioEncryption"/>
869         <xs:element ref="MobileNetworkEndToEndEncryption"/>
870         <xs:element ref="WTLS"/>
871         <xs:element ref="IPSec"/>
872         <xs:element ref="PSTN"/>
873         <xs:element ref="ISDN"/>
874         <xs:element ref="ADSL"/>
875         <xs:element ref="Extension" maxOccurs="unbounded"/>
876     </xs:choice>
877 </xs:complexType>
878
879 <xs:complexType name="PrincipalAuthenticationMechanismType">
880     <xs:sequence>
881         <xs:choice>
882             <xs:element ref="Password"/>
883             <xs:element ref="Token"/>
884             <xs:element ref="Smartcard"/>
885             <xs:element ref="ActivationPin"/>
886             <xs:element ref="Extension" maxOccurs="unbounded"/>
887         </xs:choice>
888     </xs:sequence>
889     <xs:attribute name="preauth" type="xs:integer"
890 use="optional"/>
891 </xs:complexType>
892

```

```

893 <xs:complexType name="AuthnMethodBaseType">
894   <xs:sequence>
895     <xs:element ref="PrincipalAuthenticationMechanism"
896       minOccurs="0"/>
897     <xs:element ref="Authenticator" minOccurs="0"/>
898     <xs:element ref="AuthenticatorTransportProtocol"
899       minOccurs="0"/>
900     <xs:element ref="Extension" minOccurs="0"
901       maxOccurs="unbounded"/>
902   </xs:sequence>
903 </xs:complexType>
904
905 <xs:complexType name="AuthnContextDeclarationBaseType">
906   <xs:sequence>
907     <xs:element ref="Identification" minOccurs="0"/>
908     <xs:element ref="TechnicalProtection" minOccurs="0"/>
909     <xs:element ref="OperationalProtection" minOccurs="0"/>
910     <xs:element ref="AuthenticationMethod" minOccurs="0"/>
911     <xs:element ref="GoverningAgreements" minOccurs="0"/>
912     <xs:element ref="AuthenticatingAuthority" minOccurs="0"
913       maxOccurs="unbounded"/>
914     <xs:element ref="Extension" minOccurs="0"
915       maxOccurs="unbounded"/>
916   </xs:sequence>
917   <xs:attribute name="ID" type="xs:ID"/>
918 </xs:complexType>
919
920 <xs:complexType name="TechnicalProtectionBaseType">
921   <xs:choice>
922     <xs:element ref="PrivateKeyProtection" minOccurs="0"/>
923     <xs:element ref="SecretKeyProtection" minOccurs="0"/>
924     <xs:element ref="Extension" minOccurs="0"
925       maxOccurs="unbounded"/>
926   </xs:choice>
927 </xs:complexType>
928
929 <xs:complexType name="OperationalProtectionType">
930   <xs:sequence>
931     <xs:element ref="SecurityAudit" minOccurs="0"/>
932     <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
933     <xs:element ref="Extension" minOccurs="0"
934       maxOccurs="unbounded"/>
935   </xs:sequence>
936 </xs:complexType>
937
938 <xs:complexType name="AuthenticatorBaseType">
939   <xs:choice>
940     <xs:element ref="PreviousSession"/>
941     <xs:element ref="ResumeSession"/>
942     <xs:element ref="DigSig"/>
943     <xs:element ref="Password"/>
944     <xs:element ref="ZeroKnowledge"/>
945     <xs:element ref="SharedSecretChallengeResponse"/>
946     <xs:element ref="SharedSecretDynamicPlaintext"/>
947     <xs:element ref="IPAddress"/>
948     <xs:element ref="AsymmetricDecryption"/>
949     <xs:element ref="AsymmetricKeyAgreement"/>
950     <xs:element ref="SubscriberLineNumber"/>
951     <xs:element ref="UserSuffix"/>
952     <xs:element ref="Extension" maxOccurs="unbounded"/>
953   </xs:choice>

```

```

954 </xs:complexType>
955
956 <xs:complexType name="KeyActivationType">
957   <xs:choice>
958     <xs:element ref="ActivationPin"/>
959     <xs:element ref="Extension" maxOccurs="unbounded"/>
960   </xs:choice>
961 </xs:complexType>
962
963 <xs:complexType name="KeySharingType">
964   <xs:attribute name="sharing" type="xs:boolean"
965     use="required"/>
966 </xs:complexType>
967
968 <xs:complexType name="PrivateKeyProtectionType">
969   <xs:sequence>
970     <xs:element ref="KeyActivation" minOccurs="0"/>
971     <xs:element ref="KeyStorage" minOccurs="0"/>
972     <xs:element ref="KeySharing" minOccurs="0"/>
973     <xs:element ref="Extension" minOccurs="0"
974       maxOccurs="unbounded"/>
975   </xs:sequence>
976 </xs:complexType>
977
978 <xs:complexType name="PasswordType">
979   <xs:sequence>
980     <xs:element ref="Length" minOccurs="0"/>
981     <xs:element ref="Alphabet" minOccurs="0"/>
982     <xs:element ref="Generation" minOccurs="0"/>
983     <xs:element ref="Extension" minOccurs="0"
984       maxOccurs="unbounded"/>
985   </xs:sequence>
986   <xs:attribute name="ExternalVerification" type="xs:anyURI"
987 use="optional"/>
988 </xs:complexType>
989
990 <xs:element name="RestrictedPassword"
991 type="RestrictedPasswordType"/>
992
993 <xs:complexType name="RestrictedPasswordType">
994   <xs:complexContent>
995     <xs:restriction base="PasswordType">
996       <xs:sequence>
997         <xs:element ref="RestrictedLength" minOccurs="1"/>
998         <xs:element ref="Generation" minOccurs="0"/>
999         <xs:element ref="Extension" minOccurs="0"
1000 maxOccurs="unbounded"/>
1001       </xs:sequence>
1002       <xs:attribute name="ExternalVerification"
1003 type="xs:anyURI" use="optional"/>
1004     </xs:restriction>
1005   </xs:complexContent>
1006 </xs:complexType>
1007
1008 <xs:element name="RestrictedLength"
1009 type="RestrictedLengthType"/>
1010
1011 <xs:complexType name="RestrictedLengthType">
1012   <xs:complexContent>
1013     <xs:restriction base="LengthType">
1014       <xs:attribute name="min" use="required">

```

```

1015         <xs:simpleType>
1016             <xs:restriction base="xs:integer">
1017                 <xs:minInclusive value="3"/>
1018             </xs:restriction>
1019         </xs:simpleType>
1020     </xs:attribute>
1021     <xs:attribute name="max" type="xs:integer"
1022 use="optional"/>
1023 </xs:restriction>
1024 </xs:complexContent>
1025 </xs:complexType>
1026
1027 <xs:complexType name="ActivationPinType">
1028     <xs:sequence>
1029         <xs:element ref="Length" minOccurs="0"/>
1030         <xs:element ref="Alphabet" minOccurs="0"/>
1031         <xs:element ref="Generation" minOccurs="0"/>
1032         <xs:element ref="ActivationLimit" minOccurs="0"/>
1033         <xs:element ref="Extension" minOccurs="0"
1034             maxOccurs="unbounded"/>
1035     </xs:sequence>
1036 </xs:complexType>
1037 <xs:element name="Alphabet" type="AlphabetType"/>
1038 <xs:complexType name="AlphabetType">
1039     <xs:attribute name="requiredChars" type="xs:string"
1040 use="required"/>
1041     <xs:attribute name="excludedChars" type="xs:string"
1042 use="optional"/>
1043     <xs:attribute name="case" type="xs:string" use="optional"/>
1044 </xs:complexType>
1045 <xs:complexType name="TokenType">
1046     <xs:sequence>
1047         <xs:element ref="TimeSyncToken"/>
1048         <xs:element ref="Extension" minOccurs="0"
1049             maxOccurs="unbounded"/>
1050     </xs:sequence>
1051 </xs:complexType>
1052 <xs:complexType name="TimeSyncTokenType">
1053     <xs:attribute name="DeviceType" use="required">
1054         <xs:simpleType>
1055             <xs:restriction base="xs:NMTOKEN">
1056                 <xs:enumeration value="hardware"/>
1057                 <xs:enumeration value="software"/>
1058             </xs:restriction>
1059         </xs:simpleType>
1060     </xs:attribute>
1061     <xs:attribute name="SeedLength" type="xs:integer"
1062 use="required"/>
1063     <xs:attribute name="DeviceInHand" use="required">
1064         <xs:simpleType>
1065             <xs:restriction base="xs:NMTOKEN">
1066                 <xs:enumeration value="true"/>
1067                 <xs:enumeration value="false"/>
1068             </xs:restriction>
1069         </xs:simpleType>
1070     </xs:attribute>
1071 </xs:complexType>
1072 <xs:complexType name="ActivationLimitType">
1073     <xs:choice>
1074         <xs:element ref="ActivationLimitDuration"/>
1075         <xs:element ref="ActivationLimitUsages"/>

```

```

1076     <xs:element ref="ActivationLimitSession"/>
1077   </xs:choice>
1078 </xs:complexType>
1079 <xs:element name="ActivationLimitDuration"
1080   type="ActivationLimitDurationType">
1081   <xs:annotation>
1082     <xs:documentation>
1083       This element indicates that the Key Activation Limit is
1084       defined as a specific duration of time.
1085     </xs:documentation>
1086   </xs:annotation>
1087 </xs:element>
1088 <xs:element name="ActivationLimitUsages"
1089   type="ActivationLimitUsagesType">
1090   <xs:annotation>
1091     <xs:documentation>
1092       This element indicates that the Key Activation Limit is
1093       defined as a number of usages.
1094     </xs:documentation>
1095   </xs:annotation>
1096 </xs:element>
1097 <xs:element name="ActivationLimitSession"
1098   type="ActivationLimitSessionType">
1099   <xs:annotation>
1100     <xs:documentation>
1101       This element indicates that the Key Activation Limit is
1102       the session.
1103     </xs:documentation>
1104   </xs:annotation>
1105 </xs:element>
1106 <xs:complexType name="ActivationLimitDurationType">
1107   <xs:attribute name="duration" type="xs:duration"
1108     use="required"/>
1109 </xs:complexType>
1110 <xs:complexType name="ActivationLimitUsagesType">
1111   <xs:attribute name="number" type="xs:integer"
1112     use="required"/>
1113 </xs:complexType>
1114 <xs:complexType name="ActivationLimitSessionType"/>
1115 <xs:complexType name="LengthType">
1116   <xs:attribute name="min" type="xs:integer" use="required"/>
1117   <xs:attribute name="max" type="xs:integer" use="optional"/>
1118 </xs:complexType>
1119
1120 <xs:complexType name="KeyStorageType">
1121   <xs:attribute name="medium" use="required">
1122     <xs:simpleType>
1123       <xs:restriction base="xs:NMTOKEN">
1124         <xs:enumeration value="memory"/>
1125         <xs:enumeration value="smartcard"/>
1126         <xs:enumeration value="token"/>
1127         <xs:enumeration value="MobileDevice"/>
1128         <xs:enumeration value="MobileAuthCard"/>
1129       </xs:restriction>
1130     </xs:simpleType>
1131   </xs:attribute>
1132 </xs:complexType>
1133
1134 <xs:complexType name="SecretKeyProtectionType">
1135   <xs:sequence>
1136     <xs:element ref="KeyActivation" minOccurs="0"/>

```

```
1137     <xs:element ref="KeyStorage" minOccurs="0"/>
1138     <xs:element ref="Extension" maxOccurs="unbounded"/>
1139   </xs:sequence>
1140 </xs:complexType>
1141
1142 <xs:complexType name="SecurityAuditType">
1143   <xs:sequence>
1144     <xs:element ref="SwitchAudit" minOccurs="0"/>
1145     <xs:element ref="Extension" minOccurs="0"
1146       maxOccurs="unbounded"/>
1147   </xs:sequence>
1148 </xs:complexType>
1149
1150 <xs:element name="Extension" type="ExtensionType"/>
1151
1152 <xs:complexType name="ExtensionType">
1153   <xs:sequence>
1154     <xs:any namespace="##other" processContents="lax"
1155 maxOccurs="unbounded"/>
1156   </xs:sequence>
1157 </xs:complexType>
1158
1159 </xs:schema>
```

1160 3 Authentication Context Classes

1161 The number of permutations of the different authentication context characteristics ensure that there are a
1162 theoretically infinite number of unique authentication contexts. The implication is that in theory any
1163 particular relying party would be expected to be able to parse arbitrary authentication context declarations
1164 and, more importantly, to analyze the declaration in order to assess the 'quality' of the associated
1165 authentication assertion. Making such an assessment is non-trivial.

1166 Fortunately, an optimization is possible. While theoretically infinite, in practice many authentication
1167 contexts will fall into categories - these categories determined by industry practices and technology. For
1168 instance, many B2C Web browser authentication contexts will be (partially) defined by the Principal
1169 authenticating to the authentication authority through the presentation of a password over an SSL
1170 protected session. In the enterprise world, certificate-based authentication will be more common. Of
1171 course, the full authentication context is not limited to the specifics of how the Principal authenticated.
1172 Nevertheless, the authentication method is often the most *visible* characteristic and as such, can serve as
1173 a useful classifier for a class of related authentication contexts.

1174 The OASIS SSTC normalizes this concept through the definition of a number of *Authentication Context*
1175 *Classes*. Each class will define a proper subset of the full set of authentication contexts. Classes have
1176 been chosen as representative of the current practices and technologies for authentication technologies.
1177 Classes will provide identity and service providers a convenient shorthand when referring to authentication
1178 context issues. For instance, an authentication authority, may include with the complete authentication
1179 context declaration it provides to a service provider an assertion that the authentication context also
1180 belongs to one of the SSTC defined authentication classes. For some service providers, this assertion will
1181 be sufficient detail for it to be able to assign an appropriate level of confidence to the associated
1182 authentication assertion. Other service providers might prefer to examine the complete authentication
1183 context declaration itself. Likewise, the ability to refer to an authentication context class rather than being
1184 required to list the complete details of a specific authentication content will simplify how the service
1185 provider expresses its desires and/or requirements to an authentication authority.

1186 3.1 Advantages of Authentication Context Classes

1187 The introduction of the additional layer of classes and the definition of an initial list of representative and
1188 flexible classes are expected to:

- 1189 • Make it easier for the authentication authority and service provider to come to an agreement on what
1190 are acceptable authentication contexts by giving them a framework for discussion.
- 1191 • Make it easier for service providers to indicate their preferences when requesting a step-up
1192 authentication assertion from an authentication authority.
- 1193 • Simplify for service providers the burden of processing authentication context declarations by giving
1194 them the option of being satisfied by the associated class.
- 1195 • Protect service providers from impact of new authentication technologies.
- 1196 • Make it easier for authentication authorities to publish their authentication capabilities, for example,
1197 through WSDL.

1198 3.2 Processing Rules

1199 Further processing rules for authentication context classes are described in the SAML assertions and
1200 protocols specification [SAMLCore].

1200 3.3 Extensibility

1201 As does the core Authentication Context Declaration schema, the separate Authentication Context
1202 Classes schemas allow the `<Extension>` element in certain locations of the tree structure. In general,
1203 where the `<Extension>` element occurred as a child of a `<Choice>` element, this option was removed
1204 in creating the appropriate class schema definition as an extension of the base type. When the
1205 `<Extension>` element occurred as an optional child of a `<Sequence>` element, the `<Extension>`
1206 element was allowed to remain in addition to any required elements.

1207 Consequently, authentication context declarations can include the `<Extension>` element (with additional
1208 elements in different namespaces) and still conform to authentication context class schemas (if they meet
1209 the other requirements of the schema of course)

1210 The Authentication Context Class schemas extend (as restrictions) appropriate type definitions in the core
1211 Authentication Context Declaration schema. As an extension point, the Authentication Context Classes
1212 schemas themselves can be extended - their type definitions serving as base types in some other schema
1213 (potentially defined by some community wishing a more tightly defined authentication context class). To
1214 prevent logical inconsistencies, any such extensions can only further constrain the type definitions of the
1215 core Authentication Context Declaration schema. To enforce this constraint, the Authentication Context
1216 Class schemas are defined with the `finalDefault="extension"` attribute on the `<schema>` element
1217 to prevent this type of extension derivation.

1218 Additional authentication context classes MAY be developed by groups other than the SSTC. OASIS
1219 members may wish to document and submit them for consideration by the SSTC in a future version of the
1220 specification, and other groups may simply wish to inform the committee of their work. Please refer to the
1221 SSTC web site for further details.

1222 Guidelines for the specification of new context classes are as follows:

- 1223 • Specify a URI that uniquely identifies the context class.
- 1224 • Provide contact information for the author of the class.
- 1225 • Provide a textual description of the circumstances under which this class should be used.
- 1226 • Provide a valid XML schema [XMLSchema] document implementing the class

1227 Authors of new classes are encouraged to review those classes defined within this specification in order to
1228 guide their work.

1229 3.4 Schemas

1230 The SSTC-defined authentication context classes are listed in the following subsections. The classes are
1231 listed in alphabetical order; no other ranking is implied by the order of classes. Classes are uniquely
1232 identified by URIs with the following initial stem:

1233 `urn:oasis:names:tc:SAML:2.0:ac:classes`

1234 The class schemas are defined as extension by restriction of parts of the the base Authentication Context
1235 schema. XML instances that validate against a given authentication context class schema are said to
1236 *conform* to that authentication context class.

1237 3.4.1 Internet Protocol

1238 **URI:** `urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol`

1239 The Internet Protocol class is identified when a Principal is authenticated through the use of a provided IP
1240 address.

1241 `<?xml version="1.0" encoding="UTF-8"?>`
1242

```

1243 <xs:schema
1244 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1245   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1246   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1247   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1248   finalDefault="extension">
1249
1250   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1251   schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1252
1253   <xs:annotation>
1254     <xs:documentation>
1255       urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
1256     </xs:documentation>
1257   </xs:annotation>
1258
1259   <xs:complexType name="AuthnContextDeclaration">
1260     <xs:complexContent>
1261       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1262         <xs:sequence>
1263           <xs:element ref="ac:Identification" minOccurs="0"/>
1264           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
1265           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
1266           <xs:element ref="AuthnMethod"/>
1267           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1268           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1269             maxOccurs="unbounded"/>
1270           <xs:element ref="ac:Extension" minOccurs="0"
1271             maxOccurs="unbounded"/>
1272         </xs:sequence>
1273         <xs:attribute name="ID" type="xs:ID"/>
1274       </xs:restriction>
1275     </xs:complexContent>
1276   </xs:complexType>
1277
1278   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1279
1280   <xs:complexType name="AuthnMethodType">
1281     <xs:complexContent>
1282       <xs:restriction base="ac:AuthnMethodBaseType">
1283         <xs:sequence>
1284           <xs:element ref="ac:PrincipalAuthenticationMechanism"
1285             minOccurs="0"/>
1286           <xs:element ref="Authenticator"/>
1287           <xs:element ref="ac:AuthenticatorTransportProtocol"
1288             minOccurs="0"/>
1289           <xs:element ref="ac:Extension" minOccurs="0"
1290             maxOccurs="unbounded"/>
1291         </xs:sequence>
1292       </xs:restriction>
1293     </xs:complexContent>
1294   </xs:complexType>
1295
1296   <xs:element name="Authenticator" type="InternetProtocolType"/>
1297
1298   <xs:complexType name="InternetProtocolType">
1299     <xs:complexContent>
1300       <xs:restriction base="ac:AuthenticatorBaseType">
1301         <xs:choice>
1302           <xs:element ref="ac:IPAddress"/>
1303         </xs:choice>
1304       </xs:restriction>
1305     </xs:complexContent>
1306   </xs:complexType>
1307
1308 </xs:schema>

```

1309 3.4.2 InternetProtocolPassword

1310 URI: urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword

1311 The Internet Protocol Password class is identified when a Principal is authenticated through the use of a
1312 provided IP address, in addition to username/password.

```
1313 <?xml version="1.0" encoding="UTF-8"?>
1314
1315 <xs:schema
1316 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolP
1317 assword"
1318 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1319 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1320 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
1321 finalDefault="extension">
1322
1323   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1324 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1325
1326   <xs:annotation>
1327     <xs:documentation>
1328       urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
1329     </xs:documentation>
1330   </xs:annotation>
1331
1332   <xs:complexType name="AuthnContextDeclaration">
1333     <xs:complexContent>
1334       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1335         <xs:sequence>
1336           <xs:element ref="ac:Identification" minOccurs="0"/>
1337           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
1338           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
1339           <xs:element ref="AuthnMethod"/>
1340           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1341           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1342             maxOccurs="unbounded"/>
1343           <xs:element ref="ac:Extension" minOccurs="0"
1344             maxOccurs="unbounded"/>
1345         </xs:sequence>
1346         <xs:attribute name="ID" type="xs:ID"/>
1347       </xs:restriction>
1348     </xs:complexContent>
1349   </xs:complexType>
1350
1351   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1352
1353   <xs:complexType name="AuthnMethodType">
1354     <xs:complexContent>
1355       <xs:restriction base="ac:AuthnMethodBaseType">
1356         <xs:sequence>
1357           <xs:element ref="ac:PrincipalAuthenticationMechanism"
1358             minOccurs="0"/>
1359           <xs:element ref="Authenticator"/>
1360           <xs:element ref="ac:AuthenticatorTransportProtocol"
1361             minOccurs="0"/>
1362           <xs:element ref="ac:Extension" minOccurs="0"
1363             maxOccurs="unbounded"/>
1364         </xs:sequence>
1365       </xs:restriction>
1366     </xs:complexContent>
1367   </xs:complexType>
1368
1369   <xs:element name="Authenticator" type="InternetProtocolType"/>
1370
1371   <xs:complexType name="InternetProtocolType">
1372     <xs:complexContent>
```

```

1373     <xs:restriction base="ac:AuthenticatorBaseType">
1374         <xs:sequence>
1375             <xs:element ref="ac:IPAddress"/>
1376             <xs:element ref="ac:Password"/>
1377             <xs:element ref="ac:Extension" minOccurs="0"
1378                 maxOccurs="unbounded"/>
1379         </xs:sequence>
1380     </xs:restriction>
1381 </xs:complexContent>
1382 </xs:complexType>
1383
1384 </xs:schema>

```

1385 3.4.3 Kerberos

1386 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

1387 This class is defined for use when the Principal has authenticated using a password to a local
1388 authentication authority, in order to acquire a Kerberos ticket. That Kerberos ticket is then used for
1389 subsequent network authentication.

1390 **Note:** It is possible for the authentication authority to indicate (via this context class) any
1391 pre-authentication method used by the Kerberos Key Distribution Center [RFC1510] in
1392 authenticating the Principal. How the authentication authority obtains this information is
1393 outside of the scope of this specification, but it is strongly recommended that a trusted
1394 method be deployed to pass the pre-authentication type and any other Kerberos related
1395 context details to the authentication authority.

```

1396 <?xml version="1.0" encoding="UTF-8"?>
1397
1398 <xs:schema
1399 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1400 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1401 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1402 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1403 finalDefault="extension">
1404
1405     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1406     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1407
1408     <xs:annotation>
1409         <xs:documentation>
1410             urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
1411         </xs:documentation>
1412     </xs:annotation>
1413
1414     <xs:complexType name="AuthnContextDeclaration">
1415         <xs:complexContent>
1416             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1417                 <xs:sequence>
1418                     <xs:element ref="ac:Identification" minOccurs="0"/>
1419                     <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
1420                     <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
1421                     <xs:element ref="AuthnMethod"/>
1422                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1423                     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1424                         maxOccurs="unbounded"/>
1425                     <xs:element ref="ac:Extension" minOccurs="0"
1426                         maxOccurs="unbounded"/>
1427                 </xs:sequence>
1428                 <xs:attribute name="ID" type="xs:ID"/>
1429             </xs:restriction>
1430         </xs:complexContent>
1431     </xs:complexType>
1432
1433

```

```

1433 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1434
1435 <xs:complexType name="AuthnMethodType">
1436 <xs:complexContent>
1437 <xs:restriction base="ac:AuthnMethodBaseType">
1438 <xs:sequence>
1439 <xs:element ref="AuthnMechanism"/>
1440 <xs:element ref="Authenticator"/>
1441 <xs:element ref="ac:AuthenticatorTransportProtocol"
1442 minOccurs="0"/>
1443 <xs:element ref="ac:Extension" minOccurs="0"
1444 maxOccurs="unbounded"/>
1445 </xs:sequence>
1446 </xs:restriction>
1447 </xs:complexContent>
1448 </xs:complexType>
1449
1450 <xs:element name="AuthnMechanism" type="PasswordAuthnMechanismType"/>
1451
1452 <xs:complexType name="PasswordAuthnMechanismType">
1453 <xs:complexContent>
1454 <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
1455 <xs:sequence>
1456 <xs:choice>
1457 <xs:element ref="ac:RestrictedPassword"/>
1458 </xs:choice>
1459 </xs:sequence>
1460 <xs:attribute name="preauth" type="xs:integer" use="optional"/>
1461 </xs:restriction>
1462 </xs:complexContent>
1463 </xs:complexType>
1464
1465 <xs:element name="Authenticator" type="SharedSecretType"/>
1466
1467 <xs:complexType name="SharedSecretType">
1468 <xs:complexContent>
1469 <xs:restriction base="ac:AuthenticatorBaseType">
1470 <xs:choice>
1471 <xs:element ref="SharedSecretChallengeResponse"/>
1472 </xs:choice>
1473 </xs:restriction>
1474 </xs:complexContent>
1475 </xs:complexType>
1476
1477 <xs:element name="SharedSecretChallengeResponse"
1478 type="ChallengeResponseType"/>
1479
1480 <xs:complexType name="ChallengeResponseType">
1481 <xs:complexContent>
1482 <xs:restriction base="ac:SharedSecretChallengeResponseType">
1483 <xs:attribute name="method"
1484 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos"/>
1485 </xs:restriction>
1486 </xs:complexContent>
1487 </xs:complexType>
1488
1489 </xs:schema>

```

1490 An example of an XML instance conforming to this class schema is as follows:

```

1491 <?xml version="1.0" encoding="UTF-8"?>
1492
1493 <AuthnContextDeclaration
1494 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1495 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1496 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos">
1497
1498 <AuthnMethod>

```

```

1499         <PasswordAuthnMechanism preauth="0">
1500             <ac:Password/>
1501         </PasswordAuthnMechanism>
1502     </AuthnMethod>
1503 </AuthnContextDeclaration>
1504
1505     <Authenticator>
1506         <SharedSecretChallengeResponse
1507             method="urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos"/>
1508     </Authenticator>
1509 </AuthnMethod>
1510 </AuthnContextDeclaration>
1511
1512
1513
1514
1515

```

1516 3.4.4 MobileOneFactorUnregistered

1517 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered

1518 Reflects no mobile customer registration procedures and an authentication of the mobile device without
1519 requiring explicit end-user interaction. Again, this context authenticates only the device and never the user,
1520 it is useful when services other than the mobile operator want to add a secure device authentication to
1521 their authentication process.

```

1522 <?xml version="1.0" encoding="UTF-8"?>
1523
1524 <xs:schema
1525     targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUn
1526     registered"
1527     xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1528     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1529     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregister
1530     ed"
1531     finalDefault="extension">
1532
1533     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1534     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1535
1536     <xs:annotation>
1537         <xs:documentation>
1538             urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
1539         </xs:documentation>
1540     </xs:annotation>
1541
1542     <xs:complexType name="AuthnContextDeclaration">
1543         <xs:complexContent>
1544             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1545                 <xs:sequence>
1546                     <xs:element ref="Identification" minOccurs="0"/>
1547                     <xs:element ref="TechnicalProtection" minOccurs="0"/>
1548                     <xs:element ref="OperationalProtection" minOccurs="0"/>
1549                     <xs:element ref="AuthnMethod"/>
1550                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1551                     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1552                     maxOccurs="unbounded"/>
1553                     <xs:element ref="ac:Extension" minOccurs="0"
1554                     maxOccurs="unbounded"/>
1555                 </xs:sequence>
1556                 <xs:attribute name="ID" type="xs:ID"/>
1557             </xs:restriction>
1558         </xs:complexContent>
1559     </xs:complexType>
1560

```

```

1561 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1562
1563 <xs:complexType name="AuthnMethodType">
1564 <xs:complexContent>
1565 <xs:restriction base="ac:AuthnMethodBaseType">
1566 <xs:sequence>
1567 <xs:element ref="ac:PrincipalAuthenticationMechanism"
1568 minOccurs="0"/>
1569 <xs:element ref="Authenticator"/>
1570 <xs:element ref="AuthenticatorTransportProtocol"
1571 minOccurs="0"/>
1572 <xs:element ref="ac:Extension" minOccurs="0"
1573 maxOccurs="unbounded"/>
1574 </xs:sequence>
1575 </xs:restriction>
1576 </xs:complexContent>
1577 </xs:complexType>
1578
1579 <xs:element name="Authenticator" type="AuthenticatorType"/>
1580
1581 <xs:complexType name="AuthenticatorType">
1582 <xs:complexContent>
1583 <xs:restriction base="ac:AuthenticatorBaseType">
1584 <xs:choice>
1585 <xs:element ref="ac:DigSig"/>
1586 <xs:element ref="ac:ZeroKnowledge"/>
1587 <xs:element ref="ac:SharedSecretChallengeResponse"/>
1588 <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
1589 <xs:element ref="ac:AsymmetricDecryption"/>
1590 <xs:element ref="ac:AsymmetricKeyAgreement"/>
1591 </xs:choice>
1592 </xs:restriction>
1593 </xs:complexContent>
1594 </xs:complexType>
1595
1596 <xs:element name="AuthenticatorTransportProtocol"
1597 type="SecureTransportType"/>
1598
1599 <xs:complexType name="SecureTransportType">
1600 <xs:complexContent>
1601 <xs:restriction base="ac:AuthenticatorTransportProtocolType">
1602 <xs:choice>
1603 <xs:element ref="ac:SSL"/>
1604 <xs:element ref="ac:MobileNetworkRadioEncryption"/>
1605 <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
1606 <xs:element ref="ac:WTLS"/>
1607 </xs:choice>
1608 </xs:restriction>
1609 </xs:complexContent>
1610 </xs:complexType>
1611
1612 <xs:element name="OperationalProtection"
1613 type="OperationalProtectionType"/>
1614
1615 <xs:complexType name="OperationalProtectionType">
1616 <xs:complexContent>
1617 <xs:restriction base="OperationalProtectionType">
1618 <xs:sequence>
1619 <xs:element ref="ac:SecurityAudit"/>
1620 <xs:element ref="ac:DeactivationCallCenter"/>
1621 <xs:element ref="ac:Extension" minOccurs="0"
1622 maxOccurs="unbounded"/>
1623 </xs:sequence>
1624 </xs:restriction>
1625 </xs:complexContent>
1626 </xs:complexType>
1627

```

```

1628 <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
1629
1630 <xs:complexType name="TechnicalProtectionType">
1631   <xs:complexContent>
1632     <xs:restriction base="ac:TechnicalProtectionBaseType">
1633       <xs:choice>
1634         <xs:element ref="PrivateKeyProtection"/>
1635         <xs:element ref="SecretKeyProtection"/>
1636       </xs:choice>
1637     </xs:restriction>
1638   </xs:complexContent>
1639 </xs:complexType>
1640
1641 <xs:element name="PrivateKeyProtection"
1642 type="PrivateKeyProtectionType"/>
1643
1644 <xs:complexType name="PrivateKeyProtectionType">
1645   <xs:complexContent>
1646     <xs:restriction base="ac:PrivateKeyProtectionType">
1647       <xs:sequence>
1648         <xs:element ref="KeyStorage"/>
1649         <xs:element ref="ac:Extension" minOccurs="0"
1650 maxOccurs="unbounded"/>
1651       </xs:sequence>
1652     </xs:restriction>
1653   </xs:complexContent>
1654 </xs:complexType>
1655
1656 <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>
1657
1658 <xs:complexType name="SecretKeyProtectionType">
1659   <xs:complexContent>
1660     <xs:restriction base="ac:SecretKeyProtectionType">
1661       <xs:sequence>
1662         <xs:element ref="KeyStorage"/>
1663         <xs:element ref="ac:Extension" minOccurs="0"
1664 maxOccurs="unbounded"/>
1665       </xs:sequence>
1666     </xs:restriction>
1667   </xs:complexContent>
1668 </xs:complexType>
1669
1670 <xs:element name="KeyStorage" type="KeyStorageType"/>
1671
1672 <xs:complexType name="KeyStorageType">
1673   <xs:complexContent>
1674     <xs:restriction base="ac:KeyStorageType">
1675       <xs:attribute name="medium" use="required">
1676         <xs:simpleType>
1677           <xs:restriction base="xs:NMTOKEN">
1678             <xs:enumeration value="MobileDevice"/>
1679             <xs:enumeration value="MobileAuthCard"/>
1680             <xs:enumeration value="smartcard"/>
1681           </xs:restriction>
1682         </xs:simpleType>
1683       </xs:attribute>
1684     </xs:restriction>
1685   </xs:complexContent>
1686 </xs:complexType>
1687
1688 <xs:element name="SecurityAudit" type="SecurityAuditType"/>
1689
1690 <xs:complexType name="SecurityAuditType">
1691   <xs:complexContent>
1692     <xs:restriction base="ac:SecurityAuditType">
1693       <xs:sequence>
1694         <xs:element ref="ac:SwitchAudit"/>

```

```

1695         <xs:element ref="ac:Extension" minOccurs="0"
1696 maxOccurs="unbounded"/>
1697     </xs:sequence>
1698 </xs:restriction>
1699 </xs:complexContent>
1700 </xs:complexType>
1701
1702 <xs:element name="Identification" type="IdentificationType"/>
1703
1704 <xs:complexType name="IdentificationType">
1705     <xs:complexContent>
1706         <xs:restriction base="ac:IdentificationType">
1707             <xs:attribute name="nym">
1708                 <xs:simpleType>
1709                     <xs:restriction base="xs:NMTOKEN">
1710                         <xs:enumeration value="anonymity"/>
1711                         <xs:enumeration value="pseudonymity"/>
1712                     </xs:restriction>
1713                 </xs:simpleType>
1714             </xs:attribute>
1715         </xs:restriction>
1716     </xs:complexContent>
1717 </xs:complexType>
1718
1719 </xs:schema>

```

1720 3.4.5 MobileTwoFactorUnregistered

1721 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered

1722 Reflects no mobile customer registration procedures and a two-factor based authentication, such as
1723 secure device and user PIN. This context class is useful when a service other than the mobile operator
1724 wants to link their customer ID to a mobile supplied two-factor authentication service by capturing mobile
1725 phone data at enrollment.

```

1726 <?xml version="1.0" encoding="UTF-8"?>
1727
1728 <xs:schema
1729 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUn
1730 registered"
1731 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1732 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1733 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregister
1734 ed"
1735 finalDefault="extension">
1736
1737     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1738 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1739
1740     <xs:annotation>
1741         <xs:documentation>
1742             urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
1743         </xs:documentation>
1744     </xs:annotation>
1745
1746     <xs:complexType name="AuthnContextDeclaration">
1747         <xs:complexContent>
1748             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1749                 <xs:sequence>
1750                     <xs:element ref="Identification" minOccurs="0"/>
1751                     <xs:element ref="TechnicalProtection" minOccurs="0"/>
1752                     <xs:element ref="OperationalProtection" minOccurs="0"/>
1753                     <xs:element ref="AuthnMethod"/>
1754                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1755                     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1756 maxOccurs="unbounded"/>

```

```

1757         <xs:element ref="ac:Extension" minOccurs="0"
1758             maxOccurs="unbounded"/>
1759     </xs:sequence>
1760     <xs:attribute name="ID" type="xs:ID"/>
1761 </xs:restriction>
1762 </xs:complexContent>
1763 </xs:complexType>
1764
1765 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1766
1767 <xs:complexType name="AuthnMethodType">
1768     <xs:complexContent>
1769         <xs:restriction base="ac:AuthnMethodBaseType">
1770             <xs:sequence>
1771                 <xs:element ref="ac:PrincipalAuthenticationMechanism"
1772 minOccurs="0"/>
1773                 <xs:element ref="Authenticator"/>
1774                 <xs:element ref="AuthenticatorTransportProtocol"
1775 minOccurs="0"/>
1776                 <xs:element ref="ac:Extension" minOccurs="0"
1777                     maxOccurs="unbounded"/>
1778             </xs:sequence>
1779         </xs:restriction>
1780     </xs:complexContent>
1781 </xs:complexType>
1782
1783 <xs:element name="Authenticator" type="AuthenticatorType"/>
1784
1785 <xs:complexType name="AuthenticatorType">
1786     <xs:complexContent>
1787         <xs:restriction base="ac:AuthenticatorBaseType">
1788             <xs:choice>
1789                 <xs:element ref="ac:DigSig"/>
1790                 <xs:element ref="ac:ZeroKnowledge"/>
1791                 <xs:element ref="ac:SharedSecretChallengeResponse"/>
1792                 <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
1793                 <xs:element ref="ac:AsymmetricDecryption"/>
1794                 <xs:element ref="ac:AsymmetricKeyAgreement"/>
1795             <xs:sequence>
1796                 <xs:element ref="ac:Password" minOccurs="1"/>
1797                 <xs:choice>
1798                     <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
1799                     <xs:element ref="ac:SharedSecretChallengeResponse"/>
1800                 </xs:choice>
1801                 <xs:element ref="ac:Extension" maxOccurs="unbounded"/>
1802             </xs:sequence>
1803         </xs:choice>
1804     </xs:restriction>
1805 </xs:complexContent>
1806 </xs:complexType>
1807
1808 <xs:element name="AuthenticatorTransportProtocol"
1809 type="SecureTransportType"/>
1810
1811 <xs:complexType name="SecureTransportType">
1812     <xs:complexContent>
1813         <xs:restriction base="ac:AuthenticatorTransportProtocolType">
1814             <xs:choice>
1815                 <xs:element ref="ac:SSL"/>
1816                 <xs:element ref="ac:MobileNetworkNoEncryption"/>
1817                 <xs:element ref="ac:MobileNetworkRadioEncryption"/>
1818                 <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
1819                 <xs:element ref="ac:WTLS"/>
1820             </xs:choice>
1821         </xs:restriction>
1822     </xs:complexContent>
1823 </xs:complexType>

```

```

1824
1825     <xs:element name="OperationalProtection"
1826 type="OperationalProtectionType"/>
1827
1828     <xs:complexType name="OperationalProtectionType">
1829       <xs:complexContent>
1830         <xs:restriction base="OperationalProtectionType">
1831           <xs:sequence>
1832             <xs:element ref="ac:SecurityAudit"/>
1833             <xs:element ref="ac:DeactivationCallCenter"/>
1834             <xs:element ref="ac:Extension" minOccurs="0"
1835 maxOccurs="unbounded"/>
1836           </xs:sequence>
1837         </xs:restriction>
1838       </xs:complexContent>
1839     </xs:complexType>
1840
1841     <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
1842
1843     <xs:complexType name="TechnicalProtectionType">
1844       <xs:complexContent>
1845         <xs:restriction base="ac:TechnicalProtectionBaseType">
1846           <xs:choice>
1847             <xs:element ref="PrivateKeyProtection"/>
1848             <xs:element ref="SecretKeyProtection"/>
1849           </xs:choice>
1850         </xs:restriction>
1851       </xs:complexContent>
1852     </xs:complexType>
1853
1854     <xs:element name="PrivateKeyProtection"
1855 type="PrivateKeyProtectionType"/>
1856
1857     <xs:complexType name="PrivateKeyProtectionType">
1858       <xs:complexContent>
1859         <xs:restriction base="ac:PrivateKeyProtectionType">
1860           <xs:sequence>
1861             <xs:element ref="KeyActivation"/>
1862             <xs:element ref="KeyStorage"/>
1863             <xs:element ref="ac:Extension" minOccurs="0"
1864 maxOccurs="unbounded"/>
1865           </xs:sequence>
1866         </xs:restriction>
1867       </xs:complexContent>
1868     </xs:complexType>
1869
1870     <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>
1871
1872     <xs:complexType name="SecretKeyProtectionType">
1873       <xs:complexContent>
1874         <xs:restriction base="ac:SecretKeyProtectionType">
1875           <xs:sequence>
1876             <xs:element ref="KeyActivation"/>
1877             <xs:element ref="KeyStorage"/>
1878             <xs:element ref="ac:Extension" minOccurs="0"
1879 maxOccurs="unbounded"/>
1880           </xs:sequence>
1881         </xs:restriction>
1882       </xs:complexContent>
1883     </xs:complexType>
1884
1885     <xs:element name="KeyActivation" type="KeyActivationType"/>
1886
1887     <xs:complexType name="KeyActivationType">
1888       <xs:complexContent>
1889         <xs:restriction base="ac:KeyActivationType">
1890           <xs:sequence>

```

```

1891         <xs:element ref="ac:ActivationPin"/>
1892         <xs:element ref="ac:Extension" minOccurs="0"
1893 maxOccurs="unbounded"/>
1894     </xs:sequence>
1895 </xs:restriction>
1896 </xs:complexContent>
1897 </xs:complexType>
1898
1899     <xs:element name="KeyStorage" type="KeyStorageType"/>
1900
1901     <xs:complexType name="KeyStorageType">
1902         <xs:complexContent>
1903             <xs:restriction base="ac:KeyStorageType">
1904                 <xs:attribute name="medium" use="required">
1905                     <xs:simpleType>
1906                         <xs:restriction base="xs:NMTOKEN">
1907                             <xs:enumeration value="MobileDevice"/>
1908                             <xs:enumeration value="MobileAuthCard"/>
1909                             <xs:enumeration value="smartcard"/>
1910                         </xs:restriction>
1911                     </xs:simpleType>
1912                 </xs:attribute>
1913             </xs:restriction>
1914         </xs:complexContent>
1915     </xs:complexType>
1916
1917     <xs:element name="SecurityAudit" type="SecurityAuditType"/>
1918
1919     <xs:complexType name="SecurityAuditType">
1920         <xs:complexContent>
1921             <xs:restriction base="ac:SecurityAuditType">
1922                 <xs:sequence>
1923                     <xs:element ref="ac:SwitchAudit"/>
1924                     <xs:element ref="ac:Extension" minOccurs="0"
1925 maxOccurs="unbounded"/>
1926                 </xs:sequence>
1927             </xs:restriction>
1928         </xs:complexContent>
1929     </xs:complexType>
1930
1931     <xs:element name="Identification" type="IdentificationType"/>
1932
1933     <xs:complexType name="IdentificationType">
1934         <xs:complexContent>
1935             <xs:restriction base="ac:IdentificationType">
1936                 <xs:attribute name="nym">
1937                     <xs:simpleType>
1938                         <xs:restriction base="xs:NMTOKEN">
1939                             <xs:enumeration value="anonymity"/>
1940                             <xs:enumeration value="pseudonymity"/>
1941                         </xs:restriction>
1942                     </xs:simpleType>
1943                 </xs:attribute>
1944             </xs:restriction>
1945         </xs:complexContent>
1946     </xs:complexType>
1947
1948 </xs:schema>

```

1949 **3.4.6 MobileOneFactorContract**

1950 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract

1951 Reflects mobile contract customer registration procedures and a single factor authentication. For example,
1952 a digital signing device with tamper resistant memory for key storage, such as the mobile MSISDN, but no
1953 required PIN or biometric for real-time user authentication.

```

1954 <?xml version="1.0" encoding="UTF-8"?>
1955
1956 <xs:schema
1957 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorCo
1958 ntract"
1959   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1960   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1961   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
1962   finalDefault="extension">
1963
1964   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
1965   schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
1966
1967   <xs:annotation>
1968     <xs:documentation>
1969       urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
1970     </xs:documentation>
1971   </xs:annotation>
1972
1973   <xs:complexType name="AuthnContextDeclaration">
1974     <xs:complexContent>
1975       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
1976         <xs:sequence>
1977           <xs:element ref="Identification" minOccurs="0"/>
1978           <xs:element ref="TechnicalProtection" minOccurs="0"/>
1979           <xs:element ref="OperationalProtection" minOccurs="0"/>
1980           <xs:element ref="AuthnMethod"/>
1981           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
1982           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
1983             maxOccurs="unbounded"/>
1984           <xs:element ref="ac:Extension" minOccurs="0"
1985             maxOccurs="unbounded"/>
1986         </xs:sequence>
1987         <xs:attribute name="ID" type="xs:ID"/>
1988       </xs:restriction>
1989     </xs:complexContent>
1990   </xs:complexType>
1991
1992   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
1993
1994   <xs:complexType name="AuthnMethodType">
1995     <xs:complexContent>
1996       <xs:restriction base="ac:AuthnMethodBaseType">
1997         <xs:sequence>
1998           <xs:element ref="ac:PrincipalAuthenticationMechanism"
1999 minOccurs="0"/>
2000           <xs:element ref="Authenticator"/>
2001           <xs:element ref="AuthenticatorTransportProtocol"
2002             minOccurs="0"/>
2003           <xs:element ref="ac:Extension" minOccurs="0"
2004             maxOccurs="unbounded"/>
2005         </xs:sequence>
2006       </xs:restriction>
2007     </xs:complexContent>
2008   </xs:complexType>
2009
2010   <xs:element name="Authenticator" type="AuthenticatorType"/>
2011
2012   <xs:complexType name="AuthenticatorType">
2013     <xs:complexContent>
2014       <xs:restriction base="ac:AuthenticatorBaseType">
2015         <xs:choice>
2016           <xs:element ref="ac:DigSig"/>
2017           <xs:element ref="ac:ZeroKnowledge"/>
2018           <xs:element ref="ac:SharedSecretChallengeResponse"/>
2019           <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
2020           <xs:element ref="ac:AsymmetricDecryption"/>

```

```

2021         <xs:element ref="ac:AsymmetricKeyAgreement"/>
2022     </xs:choice>
2023 </xs:restriction>
2024 </xs:complexContent>
2025 </xs:complexType>
2026
2027     <xs:element name="AuthenticatorTransportProtocol"
2028 type="SecureTransportType"/>
2029
2030     <xs:complexType name="SecureTransportType">
2031     <xs:complexContent>
2032     <xs:restriction base="ac:AuthenticatorTransportProtocolType">
2033     <xs:choice>
2034     <xs:element ref="ac:SSL"/>
2035     <xs:element ref="ac:MobileNetworkNoEncryption"/>
2036     <xs:element ref="ac:MobileNetworkRadioEncryption"/>
2037     <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
2038     <xs:element ref="ac:WTLS"/>
2039     </xs:choice>
2040     </xs:restriction>
2041     </xs:complexContent>
2042     </xs:complexType>
2043
2044     <xs:element name="OperationalProtection"
2045 type="OperationalProtectionType"/>
2046
2047     <xs:complexType name="OperationalProtectionType">
2048     <xs:complexContent>
2049     <xs:restriction base="OperationalProtectionType">
2050     <xs:sequence>
2051     <xs:element ref="ac:SecurityAudit"/>
2052     <xs:element ref="ac:DeactivationCallCenter"/>
2053     <xs:element ref="ac:Extension" minOccurs="0"
2054 maxOccurs="unbounded"/>
2055     </xs:sequence>
2056     </xs:restriction>
2057     </xs:complexContent>
2058     </xs:complexType>
2059
2060     <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
2061
2062     <xs:complexType name="TechnicalProtectionType">
2063     <xs:complexContent>
2064     <xs:restriction base="ac:TechnicalProtectionBaseType">
2065     <xs:choice>
2066     <xs:element ref="PrivateKeyProtection"/>
2067     <xs:element ref="SecretKeyProtection"/>
2068     </xs:choice>
2069     </xs:restriction>
2070     </xs:complexContent>
2071     </xs:complexType>
2072
2073     <xs:element name="PrivateKeyProtection"
2074 type="PrivateKeyProtectionType"/>
2075
2076     <xs:complexType name="PrivateKeyProtectionType">
2077     <xs:complexContent>
2078     <xs:restriction base="ac:PrivateKeyProtectionType">
2079     <xs:sequence>
2080     <xs:element ref="KeyStorage"/>
2081     <xs:element ref="ac:Extension" minOccurs="0"
2082 maxOccurs="unbounded"/>
2083     </xs:sequence>
2084     </xs:restriction>
2085     </xs:complexContent>
2086     </xs:complexType>
2087

```

```

2088 <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>
2089
2090 <xs:complexType name="SecretKeyProtectionType">
2091 <xs:complexContent>
2092 <xs:restriction base="ac:SecretKeyProtectionType">
2093 <xs:sequence>
2094 <xs:element ref="KeyStorage"/>
2095 <xs:element ref="ac:Extension" minOccurs="0"
2096 maxOccurs="unbounded"/>
2097 </xs:sequence>
2098 </xs:restriction>
2099 </xs:complexContent>
2100 </xs:complexType>
2101
2102 <xs:element name="KeyStorage" type="KeyStorageType"/>
2103
2104 <xs:complexType name="KeyStorageType">
2105 <xs:complexContent>
2106 <xs:restriction base="ac:KeyStorageType">
2107 <xs:attribute name="medium" use="required">
2108 <xs:simpleType>
2109 <xs:restriction base="xs:NMTOKEN">
2110 <xs:enumeration value="MobileDevice"/>
2111 <xs:enumeration value="MobileAuthCard"/>
2112 <xs:enumeration value="smartcard"/>
2113 </xs:restriction>
2114 </xs:simpleType>
2115 </xs:attribute>
2116 </xs:restriction>
2117 </xs:complexContent>
2118 </xs:complexType>
2119
2120 <xs:element name="SecurityAudit" type="SecurityAuditType"/>
2121
2122 <xs:complexType name="SecurityAuditType">
2123 <xs:complexContent>
2124 <xs:restriction base="ac:SecurityAuditType">
2125 <xs:sequence>
2126 <xs:element ref="ac:SwitchAudit"/>
2127 <xs:element ref="ac:Extension" minOccurs="0"
2128 maxOccurs="unbounded"/>
2129 </xs:sequence>
2130 </xs:restriction>
2131 </xs:complexContent>
2132 </xs:complexType>
2133
2134 <xs:element name="Identification" type="IdentificationType"/>
2135
2136 <xs:complexType name="IdentificationType">
2137 <xs:complexContent>
2138 <xs:restriction base="ac:IdentificationType">
2139 <xs:sequence>
2140 <xs:element ref="ac:PhysicalVerification"/>
2141 <xs:element ref="ac:WrittenConsent"/>
2142 <xs:element ref="ac:GoverningAgreements"/>
2143 <xs:element ref="ac:Extension" minOccurs="0"
2144 maxOccurs="unbounded"/>
2145 </xs:sequence>
2146 <xs:attribute name="nym">
2147 <xs:simpleType>
2148 <xs:restriction base="xs:NMTOKEN">
2149 <xs:enumeration value="anonymity"/>
2150 <xs:enumeration value="verinyimity"/>
2151 <xs:enumeration value="pseudonymity"/>
2152 </xs:restriction>
2153 </xs:simpleType>
2154 </xs:attribute>

```

2155
2156
2157
2158
2159

```
</xs:restriction>  
</xs:complexContent>  
</xs:complexType>  
</xs:schema>
```

2160 3.4.7 MobileTwoFactorContract

2161 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract

2162 Reflects mobile contract customer registration procedures and a two-factor based authentication. For
2163 example, a digital signing device with tamper resistant memory for key storage, such as a GSM SIM, that
2164 requires explicit proof of user identity and intent, such as a PIN or biometric.

2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216

```
<?xml version="1.0" encoding="UTF-8"?>  
<xs:schema  
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorCo  
ntract"  
xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"  
xmlns:xs="http://www.w3.org/2001/XMLSchema"  
xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"  
finalDefault="extension">  
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"  
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>  
  <xs:annotation>  
    <xs:documentation>  
      urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract  
    </xs:documentation>  
  </xs:annotation>  
  <xs:complexType name="AuthnContextDeclaration">  
    <xs:complexContent>  
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">  
        <xs:sequence>  
          <xs:element ref="Identification" minOccurs="0"/>  
          <xs:element ref="TechnicalProtection" minOccurs="0"/>  
          <xs:element ref="OperationalProtection" minOccurs="0"/>  
          <xs:element ref="AuthnMethod"/>  
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>  
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"  
maxOccurs="unbounded"/>  
          <xs:element ref="ac:Extension" minOccurs="0"  
maxOccurs="unbounded"/>  
        </xs:sequence>  
        <xs:attribute name="ID" type="xs:ID"/>  
      </xs:restriction>  
    </xs:complexContent>  
  </xs:complexType>  
  <xs:element name="AuthnMethod" type="AuthnMethodType"/>  
  <xs:complexType name="AuthnMethodType">  
    <xs:complexContent>  
      <xs:restriction base="ac:AuthnMethodBaseType">  
        <xs:sequence>  
          <xs:element ref="ac:PrincipalAuthenticationMechanism"  
minOccurs="0"/>  
          <xs:element ref="Authenticator"/>  
          <xs:element ref="AuthenticatorTransportProtocol"  
minOccurs="0"/>  
          <xs:element ref="ac:Extension" minOccurs="0"  
maxOccurs="unbounded"/>  
        </xs:sequence>
```

```

2217     </xs:restriction>
2218   </xs:complexContent>
2219 </xs:complexType>
2220
2221 <xs:element name="Authenticator" type="AuthenticatorType"/>
2222
2223 <xs:complexType name="AuthenticatorType">
2224   <xs:complexContent>
2225     <xs:restriction base="ac:AuthenticatorBaseType">
2226       <xs:choice>
2227         <xs:element ref="ac:DigSig"/>
2228         <xs:element ref="ac:ZeroKnowledge"/>
2229         <xs:element ref="ac:SharedSecretChallengeResponse"/>
2230         <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
2231         <xs:element ref="ac:AsymmetricDecryption"/>
2232         <xs:element ref="ac:AsymmetricKeyAgreement"/>
2233         <xs:sequence>
2234           <xs:element ref="ac:Password" minOccurs="1"/>
2235           <xs:choice>
2236             <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
2237             <xs:element ref="ac:SharedSecretChallengeResponse"/>
2238           </xs:choice>
2239           <xs:element ref="ac:Extension" maxOccurs="unbounded"/>
2240         </xs:sequence>
2241       </xs:choice>
2242     </xs:restriction>
2243   </xs:complexContent>
2244 </xs:complexType>
2245
2246 <xs:element name="AuthenticatorTransportProtocol"
2247 type="SecureTransportType"/>
2248
2249 <xs:complexType name="SecureTransportType">
2250   <xs:complexContent>
2251     <xs:restriction base="ac:AuthenticatorTransportProtocolType">
2252       <xs:choice>
2253         <xs:element ref="ac:SSL"/>
2254         <xs:element ref="ac:MobileNetworkNoEncryption"/>
2255         <xs:element ref="ac:MobileNetworkRadioEncryption"/>
2256         <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
2257         <xs:element ref="ac:WTLS"/>
2258       </xs:choice>
2259     </xs:restriction>
2260   </xs:complexContent>
2261 </xs:complexType>
2262
2263 <xs:element name="OperationalProtection"
2264 type="OperationalProtectionType"/>
2265
2266 <xs:complexType name="OperationalProtectionType">
2267   <xs:complexContent>
2268     <xs:restriction base="OperationalProtectionType">
2269       <xs:sequence>
2270         <xs:element ref="ac:SecurityAudit"/>
2271         <xs:element ref="ac:DeactivationCallCenter"/>
2272         <xs:element ref="ac:Extension" minOccurs="0"
2273 maxOccurs="unbounded"/>
2274       </xs:sequence>
2275     </xs:restriction>
2276   </xs:complexContent>
2277 </xs:complexType>
2278
2279 <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
2280
2281 <xs:complexType name="TechnicalProtectionType">
2282   <xs:complexContent>
2283     <xs:restriction base="ac:TechnicalProtectionBaseType">

```

```

2284         <xs:choice>
2285             <xs:element ref="PrivateKeyProtection"/>
2286             <xs:element ref="SecretKeyProtection"/>
2287         </xs:choice>
2288     </xs:restriction>
2289 </xs:complexContent>
2290 </xs:complexType>
2291
2292     <xs:element name="PrivateKeyProtection"
2293 type="PrivateKeyProtectionType"/>
2294
2295     <xs:complexType name="PrivateKeyProtectionType">
2296         <xs:complexContent>
2297             <xs:restriction base="ac:PrivateKeyProtectionType">
2298                 <xs:sequence>
2299                     <xs:element ref="KeyActivation"/>
2300                     <xs:element ref="KeyStorage"/>
2301                     <xs:element ref="ac:Extension" minOccurs="0"
2302 maxOccurs="unbounded"/>
2303                 </xs:sequence>
2304             </xs:restriction>
2305         </xs:complexContent>
2306     </xs:complexType>
2307
2308     <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>
2309
2310     <xs:complexType name="SecretKeyProtectionType">
2311         <xs:complexContent>
2312             <xs:restriction base="ac:SecretKeyProtectionType">
2313                 <xs:sequence>
2314                     <xs:element ref="KeyActivation"/>
2315                     <xs:element ref="KeyStorage"/>
2316                     <xs:element ref="ac:Extension" minOccurs="0"
2317 maxOccurs="unbounded"/>
2318                 </xs:sequence>
2319             </xs:restriction>
2320         </xs:complexContent>
2321     </xs:complexType>
2322
2323     <xs:element name="KeyActivation" type="KeyActivationType"/>
2324
2325     <xs:complexType name="KeyActivationType">
2326         <xs:complexContent>
2327             <xs:restriction base="ac:KeyActivationType">
2328                 <xs:sequence>
2329                     <xs:element ref="ac:ActivationPin"/>
2330                     <xs:element ref="ac:Extension" minOccurs="0"
2331 maxOccurs="unbounded"/>
2332                 </xs:sequence>
2333             </xs:restriction>
2334         </xs:complexContent>
2335     </xs:complexType>
2336
2337     <xs:element name="KeyStorage" type="KeyStorageType"/>
2338
2339     <xs:complexType name="KeyStorageType">
2340         <xs:complexContent>
2341             <xs:restriction base="ac:KeyStorageType">
2342                 <xs:attribute name="medium" use="required">
2343                     <xs:simpleType>
2344                         <xs:restriction base="xs:NMTOKEN">
2345                             <xs:enumeration value="MobileDevice"/>
2346                             <xs:enumeration value="MobileAuthCard"/>
2347                             <xs:enumeration value="smartcard"/>
2348                         </xs:restriction>
2349                     </xs:simpleType>
2350                 </xs:attribute>

```

```

2351     </xs:restriction>
2352     </xs:complexContent>
2353 </xs:complexType>
2354
2355     <xs:element name="SecurityAudit" type="SecurityAuditType"/>
2356
2357     <xs:complexType name="SecurityAuditType">
2358     <xs:complexContent>
2359     <xs:restriction base="ac:SecurityAuditType">
2360     <xs:sequence>
2361     <xs:element ref="ac:SwitchAudit"/>
2362     <xs:element ref="ac:Extension" minOccurs="0"
2363 maxOccurs="unbounded"/>
2364     </xs:sequence>
2365     </xs:restriction>
2366     </xs:complexContent>
2367 </xs:complexType>
2368
2369     <xs:element name="Identification" type="IdentificationType"/>
2370
2371     <xs:complexType name="IdentificationType">
2372     <xs:complexContent>
2373     <xs:restriction base="ac:IdentificationType">
2374     <xs:sequence>
2375     <xs:element ref="ac:PhysicalVerification"/>
2376     <xs:element ref="ac:WrittenConsent"/>
2377     <xs:element ref="ac:GoverningAgreements"/>
2378     <xs:element ref="ac:Extension" minOccurs="0"
2379 maxOccurs="unbounded"/>
2380     </xs:sequence>
2381     <xs:attribute name="nym">
2382     <xs:simpleType>
2383     <xs:restriction base="xs:NMTOKEN">
2384     <xs:enumeration value="anonymity"/>
2385     <xs:enumeration value="veronymity"/>
2386     <xs:enumeration value="pseudonymity"/>
2387     </xs:restriction>
2388     </xs:simpleType>
2389     </xs:attribute>
2390     </xs:restriction>
2391     </xs:complexContent>
2392 </xs:complexType>
2393
2394 </xs:schema>

```

2395 3.4.8 Password

2396 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract

2397 The Password class is identified when a Principal authenticates to an authentication authority through the
2398 presentation of a password over an unprotected HTTP session.

```

2399 <?xml version="1.0" encoding="UTF-8"?>
2400
2401 <xs:schema
2402 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
2403 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2404 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2405 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
2406 finalDefault="extension">
2407
2408     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2409 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2410
2411     <xs:annotation>
2412     <xs:documentation>

```

```

2413         urn:oasis:names:tc:SAML:2.0:ac:classes:Password
2414     </xs:documentation>
2415 </xs:annotation>
2416
2417 <xs:complexType name="AuthnContextDeclaration">
2418     <xs:complexContent>
2419         <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2420             <xs:sequence>
2421                 <xs:element ref="ac:Identification" minOccurs="0"/>
2422                 <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2423                 <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
2424                 <xs:element ref="AuthnMethod"/>
2425                 <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2426                 <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
2427                     maxOccurs="unbounded"/>
2428                 <xs:element ref="ac:Extension" minOccurs="0"
2429                     maxOccurs="unbounded"/>
2430             </xs:sequence>
2431             <xs:attribute name="ID" type="xs:ID"/>
2432         </xs:restriction>
2433     </xs:complexContent>
2434 </xs:complexType>
2435
2436 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2437
2438 <xs:complexType name="AuthnMethodType">
2439     <xs:complexContent>
2440         <xs:restriction base="ac:AuthnMethodBaseType">
2441             <xs:sequence>
2442                 <xs:element ref="ac:PrincipalAuthenticationMechanism"
2443 minOccurs="0"/>
2444                 <xs:element ref="Authenticator"/>
2445                 <xs:element ref="ac:AuthenticatorTransportProtocol"
2446                     minOccurs="0"/>
2447                 <xs:element ref="ac:Extension" minOccurs="0"
2448                     maxOccurs="unbounded"/>
2449             </xs:sequence>
2450         </xs:restriction>
2451     </xs:complexContent>
2452 </xs:complexType>
2453
2454 <xs:element name="Authenticator" type="AuthenticatorType"/>
2455
2456 <xs:complexType name="AuthenticatorType">
2457     <xs:complexContent>
2458         <xs:restriction base="ac:AuthenticatorBaseType">
2459             <xs:choice>
2460                 <xs:element ref="ac:RestrictedPassword"/>
2461             </xs:choice>
2462         </xs:restriction>
2463     </xs:complexContent>
2464 </xs:complexType>
2465
2466 </xs:schema>

```

2467 Following is an example of an XML instance that conforms to the context class schema:

```

2468 <?xml version="1.0" encoding="UTF-8"?>
2469
2470     <AuthenticationContextDeclaration
2471         xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2472         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
2473         xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password">
2474
2475         <AuthnMethod>
2476             <Authenticator>
2477
2478                 <ac:RestrictedPassword>

```

```

2479         <ac:RestrictedLength min="4"/>
2480         </ac:RestrictedPassword>
2481
2482         </Authenticator>
2483     </AuthnMethod>
2484
2485 </AuthenticationContextDeclaration>

```

2486 3.4.9 PasswordProtectedTransport

2487 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport

2488 The PasswordProtectedTransport class is identified when a Principal authenticates to an authentication
2489 authority through the presentation of a password over a protected session.

```

2490 <?xml version="1.0" encoding="UTF-8"?>
2491
2492 <xs:schema
2493 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtected
2494 Transport"
2495 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2496 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2497 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport"
2498 finalDefault="extension">
2499
2500     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2501 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2502
2503
2504     <xs:annotation>
2505         <xs:documentation>
2506             urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport
2507         </xs:documentation>
2508     </xs:annotation>
2509
2510     <xs:complexType name="AuthnContextDeclaration">
2511         <xs:complexContent>
2512             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2513                 <xs:sequence>
2514                     <xs:element ref="ac:Identification" minOccurs="0"/>
2515                     <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2516                     <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
2517                     <xs:element ref="AuthnMethod"/>
2518                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2519                     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
2520 maxOccurs="unbounded"/>
2521                     <xs:element ref="ac:Extension" minOccurs="0"
2522 maxOccurs="unbounded"/>
2523                 </xs:sequence>
2524                 <xs:attribute name="ID" type="xs:ID"/>
2525             </xs:restriction>
2526         </xs:complexContent>
2527     </xs:complexType>
2528
2529     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2530
2531     <xs:complexType name="AuthnMethodType">
2532         <xs:complexContent>
2533             <xs:restriction base="ac:AuthnMethodBaseType">
2534                 <xs:sequence>
2535                     <xs:element ref="ac:PrincipalAuthenticationMechanism"
2536 minOccurs="0"/>
2537                     <xs:element ref="Authenticator"/>
2538                     <xs:element ref="AuthenticatorTransportProtocol"/>
2539                     <xs:element ref="ac:Extension" minOccurs="0"
2540 maxOccurs="unbounded"/>
2541                 </xs:sequence>

```

```

2542     </xs:restriction>
2543   </xs:complexContent>
2544 </xs:complexType>
2545
2546   <xs:element name="Authenticator" type="AuthenticatorType"/>
2547
2548   <xs:complexType name="AuthenticatorType">
2549     <xs:complexContent>
2550       <xs:restriction base="ac:AuthenticatorBaseType">
2551         <xs:choice>
2552           <xs:element ref="ac:RestrictedPassword"/>
2553         </xs:choice>
2554       </xs:restriction>
2555     </xs:complexContent>
2556   </xs:complexType>
2557
2558   <xs:element name="AuthenticatorTransportProtocol"
2559     type="SecureTransportType"/>
2560
2561   <xs:complexType name="SecureTransportType">
2562     <xs:complexContent>
2563       <xs:restriction base="ac:AuthenticatorTransportProtocolType">
2564         <xs:choice>
2565           <xs:element ref="ac:SSL"/>
2566           <xs:element ref="ac:MobileNetworkRadioEncryption"/>
2567           <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
2568           <xs:element ref="ac:WTLS"/>
2569           <xs:element ref="ac:IPSec"/>
2570         </xs:choice>
2571       </xs:restriction>
2572     </xs:complexContent>
2573   </xs:complexType>
2574
2575 </xs:schema>

```

2576 3.4.10 PreviousSession

2577 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession

2578 The PreviousSession class is identified when a Principal had authenticated to an authentication authority
2579 at some point in the past using any authentication context supported by that authentication authority.
2580 Consequently, a subsequent authentication event that the authentication authority will assert to the service
2581 provider may be significantly separated in time from the Principals current resource access request.

2582 The context for the previously authenticated session is explicitly not included in this context class because
2583 the user has not authenticated during this session, and so the mechanism that the user employed to
2584 authenticate in a previous session should not be used as part of a decision on whether to now allow
2585 access to a resource.

```

2586 <?xml version="1.0" encoding="UTF-8"?>
2587
2588 <xs:schema
2589   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2590   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2591   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2592   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2593   finalDefault="extension">
2594
2595   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2596     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2597
2598   <xs:annotation>
2599     <xs:documentation>
2600       urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
2601     </xs:documentation>

```

```

2602 </xs:annotation>
2603
2604 <xs:complexType name="AuthnContextDeclaration">
2605   <xs:complexContent>
2606     <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2607       <xs:sequence>
2608         <xs:element ref="ac:Identification" minOccurs="0"/>
2609         <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2610         <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
2611         <xs:element ref="AuthnMethod"/>
2612         <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2613         <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
2614           maxOccurs="unbounded"/>
2615         <xs:element ref="ac:Extension" minOccurs="0"
2616           maxOccurs="unbounded"/>
2617       </xs:sequence>
2618       <xs:attribute name="ID" type="xs:ID"/>
2619     </xs:restriction>
2620   </xs:complexContent>
2621 </xs:complexType>
2622
2623 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2624
2625 <xs:complexType name="AuthnMethodType">
2626   <xs:complexContent>
2627     <xs:restriction base="ac:AuthnMethodBaseType">
2628       <xs:sequence>
2629         <xs:element ref="ac:PrincipalAuthenticationMechanism"
2630           minOccurs="0"/>
2631         <xs:element ref="Authenticator"/>
2632         <xs:element ref="ac:AuthenticatorTransportProtocol"
2633           minOccurs="0"/>
2634         <xs:element ref="ac:Extension" minOccurs="0"
2635           maxOccurs="unbounded"/>
2636       </xs:sequence>
2637     </xs:restriction>
2638   </xs:complexContent>
2639 </xs:complexType>
2640
2641 <xs:element name="Authenticator" type="PreviousSessionType"/>
2642
2643 <xs:complexType name="PreviousSessionType">
2644   <xs:complexContent>
2645     <xs:restriction base="ac:AuthenticatorBaseType">
2646       <xs:choice>
2647         <xs:element ref="ac:PreviousSession"/>
2648       </xs:choice>
2649     </xs:restriction>
2650   </xs:complexContent>
2651 </xs:complexType>
2652
2653 </xs:schema>

```

2654 3.4.11 Public Key – X.509

2655 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:X509

2656 The X509 context class indicates that the Principal authenticated by means of a digital signature where
2657 the key was validated as part of an X.509 Public Key Infrastructure.

```

2658 <?xml version="1.0" encoding="UTF-8"?>
2659
2660 <xs:schema
2661 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2662 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2663 xmlns:xs="http://www.w3.org/2001/XMLSchema"

```

```

2664     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2665     finalDefault="extension">
2666
2667     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2668     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2669
2670     <xs:annotation>
2671       <xs:documentation>
2672         urn:oasis:names:tc:SAML:2.0:ac:classes:X509
2673       </xs:documentation>
2674     </xs:annotation>
2675
2676     <xs:complexType name="AuthnContextDeclaration">
2677       <xs:complexContent>
2678         <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2679           <xs:sequence>
2680             <xs:element ref="ac:Identification" minOccurs="0"/>
2681             <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2682             <xs:element ref="ac:OperationalProtection"
2683             minOccurs="0"/>
2684             <xs:element ref="AuthnMethod"/>
2685             <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2686             <xs:element ref="ac:AuthenticatingAuthority"
2687             minOccurs="0"
2688             maxOccurs="unbounded"/>
2689             <xs:element ref="ac:Extension" minOccurs="0"
2690             maxOccurs="unbounded"/>
2691           </xs:sequence>
2692           <xs:attribute name="ID" type="xs:ID"/>
2693         </xs:restriction>
2694       </xs:complexContent>
2695     </xs:complexType>
2696
2697     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2698
2699     <xs:complexType name="AuthnMethodType">
2700       <xs:complexContent>
2701         <xs:restriction base="ac:AuthnMethodBaseType">
2702           <xs:sequence>
2703             <xs:element ref="AuthnMechanism"/>
2704             <xs:element ref="Authenticator"/>
2705             <xs:element ref="ac:AuthenticatorTransportProtocol"
2706             minOccurs="0"/>
2707             <xs:element ref="ac:Extension" minOccurs="0"
2708             maxOccurs="unbounded"/>
2709           </xs:sequence>
2710         </xs:restriction>
2711       </xs:complexContent>
2712     </xs:complexType>
2713
2714     <xs:element name="AuthnMechanism"
2715     type="PasswordAuthnMechanismType"/>
2716
2717     <xs:complexType name="PasswordAuthnMechanismType">
2718       <xs:complexContent>
2719         <xs:restriction
2720         base="ac:PrincipalAuthenticationMechanismType">
2721           <xs:sequence>
2722             <xs:choice>
2723               <xs:element ref="ac:RestrictedPassword"/>
2724             </xs:choice>

```

```

2725         </xs:sequence>
2726         <xs:attribute name="preauth" type="xs:integer"
2727 use="optional"/>
2728     </xs:restriction>
2729 </xs:complexContent>
2730 </xs:complexType>
2731
2732 <xs:element name="Authenticator" type="AuthenticatorType"/>
2733
2734 <xs:complexType name="AuthenticatorType">
2735     <xs:complexContent>
2736         <xs:restriction base="ac:AuthenticatorBaseType">
2737             <xs:choice>
2738                 <xs:element ref="DigSig"/>
2739             </xs:choice>
2740         </xs:restriction>
2741     </xs:complexContent>
2742 </xs:complexType>
2743
2744 <xs:element name="DigSig" type="DigSigType"/>
2745
2746 <xs:complexType name="DigSigType">
2747     <xs:complexContent>
2748         <xs:restriction base="ac:PublicKeyType">
2749             <xs:attribute name="keyValidation"
2750 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
2751         </xs:restriction>
2752     </xs:complexContent>
2753 </xs:complexType>
2754
2755 </xs:schema>

```

2756 3.4.12 Public Key – PGP

2757 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PGP

2758 The PGP context class indicates that the Principal authenticated by means of a digital signature where the
2759 key was validated as part of a PGP Public Key Infrastructure.

```

2760 <?xml version="1.0" encoding="UTF-8"?>
2761
2762 <xs:schema
2763 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
2764 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2765 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2766 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
2767 finalDefault="extension">
2768
2769     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2770 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2771
2772     <xs:annotation>
2773         <xs:documentation>
2774             urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
2775         </xs:documentation>
2776     </xs:annotation>
2777
2778     <xs:complexType name="AuthnContextDeclaration">
2779         <xs:complexContent>
2780             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2781                 <xs:sequence>

```

```

2782         <xs:element ref="ac:Identification" minOccurs="0"/>
2783         <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2784         <xs:element ref="ac:OperationalProtection"
2785 minOccurs="0"/>
2786         <xs:element ref="AuthnMethod"/>
2787         <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2788         <xs:element ref="ac:AuthenticatingAuthority"
2789 minOccurs="0"
2790         maxOccurs="unbounded"/>
2791         <xs:element ref="ac:Extension" minOccurs="0"
2792         maxOccurs="unbounded"/>
2793     </xs:sequence>
2794     <xs:attribute name="ID" type="xs:ID"/>
2795 </xs:restriction>
2796 </xs:complexContent>
2797 </xs:complexType>
2798
2799 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2800
2801 <xs:complexType name="AuthnMethodType">
2802     <xs:complexContent>
2803         <xs:restriction base="ac:AuthnMethodBaseType">
2804             <xs:sequence>
2805                 <xs:element ref="AuthnMechanism"/>
2806                 <xs:element ref="Authenticator"/>
2807                 <xs:element ref="ac:AuthenticatorTransportProtocol"
2808                 minOccurs="0"/>
2809                 <xs:element ref="ac:Extension" minOccurs="0"
2810                 maxOccurs="unbounded"/>
2811             </xs:sequence>
2812         </xs:restriction>
2813     </xs:complexContent>
2814 </xs:complexType>
2815
2816     <xs:element name="AuthnMechanism"
2817     type="PasswordAuthnMechanismType"/>
2818
2819     <xs:complexType name="PasswordAuthnMechanismType">
2820         <xs:complexContent>
2821             <xs:restriction
2822 base="ac:PrincipalAuthenticationMechanismType">
2823                 <xs:sequence>
2824                     <xs:choice>
2825                         <xs:element ref="ac:RestrictedPassword"/>
2826                     </xs:choice>
2827                 </xs:sequence>
2828                 <xs:attribute name="preauth" type="xs:integer"
2829 use="optional"/>
2830             </xs:restriction>
2831         </xs:complexContent>
2832     </xs:complexType>
2833
2834     <xs:element name="Authenticator" type="AuthenticatorType"/>
2835
2836     <xs:complexType name="AuthenticatorType">
2837         <xs:complexContent>
2838             <xs:restriction base="ac:AuthenticatorBaseType">
2839                 <xs:choice>
2840                     <xs:element ref="DigSig"/>
2841                 </xs:choice>
2842             </xs:restriction>

```

```

2843     </xs:complexContent>
2844 </xs:complexType>
2845
2846     <xs:element name="DigSig" type="DigSigType"/>
2847
2848     <xs:complexType name="DigSigType">
2849       <xs:complexContent>
2850         <xs:restriction base="ac:PublicKeyType">
2851           <xs:attribute name="keyValidation"
2852 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
2853         </xs:restriction>
2854       </xs:complexContent>
2855     </xs:complexType>
2856
2857 </xs:schema>

```

2858 3.4.13 Public Key – SPKI

2859 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI

2860 The SPKI context class indicates that the Principal authenticated by means of a digital signature where
2861 the key was validated via an SPKI Infrastructure.

```

2862 <?xml version="1.0" encoding="UTF-8"?>
2863
2864 <xs:schema
2865 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2866 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2867 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2868 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2869 finalDefault="extension">
2870
2871   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2872 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2873
2874   <xs:annotation>
2875     <xs:documentation>
2876       urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
2877     </xs:documentation>
2878   </xs:annotation>
2879
2880   <xs:complexType name="AuthnContextDeclaration">
2881     <xs:complexContent>
2882       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2883         <xs:sequence>
2884           <xs:element ref="ac:Identification" minOccurs="0"/>
2885           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2886           <xs:element ref="ac:OperationalProtection"
2887 minOccurs="0"/>
2888           <xs:element ref="ac:AuthnMethod"/>
2889           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2890           <xs:element ref="ac:AuthenticatingAuthority"
2891 minOccurs="0"
2892           maxOccurs="unbounded"/>
2893           <xs:element ref="ac:Extension" minOccurs="0"
2894           maxOccurs="unbounded"/>
2895         </xs:sequence>
2896         <xs:attribute name="ID" type="xs:ID"/>
2897       </xs:restriction>
2898     </xs:complexContent>
2899   </xs:complexType>

```

```

2900
2901     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
2902
2903     <xs:complexType name="AuthnMethodType">
2904         <xs:complexContent>
2905             <xs:restriction base="ac:AuthnMethodBaseType">
2906                 <xs:sequence>
2907                     <xs:element ref="AuthnMechanism"/>
2908                     <xs:element ref="Authenticator"/>
2909                     <xs:element ref="ac:AuthenticatorTransportProtocol"
2910                         minOccurs="0"/>
2911                     <xs:element ref="ac:Extension" minOccurs="0"
2912                         maxOccurs="unbounded"/>
2913                 </xs:sequence>
2914             </xs:restriction>
2915         </xs:complexContent>
2916     </xs:complexType>
2917
2918     <xs:element name="AuthnMechanism"
2919         type="PasswordAuthnMechanismType"/>
2920
2921     <xs:complexType name="PasswordAuthnMechanismType">
2922         <xs:complexContent>
2923             <xs:restriction
2924                 base="ac:PrincipalAuthenticationMechanismType">
2925                 <xs:sequence>
2926                     <xs:choice>
2927                         <xs:element ref="ac:RestrictedPassword"/>
2928                     </xs:choice>
2929                 </xs:sequence>
2930                 <xs:attribute name="preauth" type="xs:integer"
2931                     use="optional"/>
2932             </xs:restriction>
2933         </xs:complexContent>
2934     </xs:complexType>
2935
2936     <xs:element name="Authenticator" type="AuthenticatorType"/>
2937
2938     <xs:complexType name="AuthenticatorType">
2939         <xs:complexContent>
2940             <xs:restriction base="ac:AuthenticatorBaseType">
2941                 <xs:choice>
2942                     <xs:element ref="DigSig"/>
2943                 </xs:choice>
2944             </xs:restriction>
2945         </xs:complexContent>
2946     </xs:complexType>
2947
2948     <xs:element name="DigSig" type="DigSigType"/>
2949
2950     <xs:complexType name="DigSigType">
2951         <xs:complexContent>
2952             <xs:restriction base="ac:PublicKeyType">
2953                 <xs:attribute name="keyValidation"
2954                     fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
2955             </xs:restriction>
2956         </xs:complexContent>
2957     </xs:complexType>
2958
2959 </xs:schema>

```

2960 3.4.14 Public Key - XML Digital Signature

2961 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig

2962 This context class indicates that the Principal authenticated by means of a digital signature according to
2963 the processing rules specified in the XML Digital Signature specification [XMLSig].

```
2964 <?xml version="1.0" encoding="UTF-8"?>
2965
2966 <xs:schema
2967 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
2968 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
2969 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2970 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
2971 finalDefault="extension">
2972
2973   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
2974 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
2975
2976   <xs:annotation>
2977     <xs:documentation>
2978       urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
2979     </xs:documentation>
2980   </xs:annotation>
2981
2982   <xs:complexType name="AuthnContextDeclaration">
2983     <xs:complexContent>
2984       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
2985         <xs:sequence>
2986           <xs:element ref="ac:Identification" minOccurs="0"/>
2987           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
2988           <xs:element ref="ac:OperationalProtection"
2989 minOccurs="0"/>
2990           <xs:element ref="AuthnMethod"/>
2991           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
2992           <xs:element ref="ac:AuthenticatingAuthority"
2993 minOccurs="0"
2994 maxOccurs="unbounded"/>
2995           <xs:element ref="ac:Extension" minOccurs="0"
2996 maxOccurs="unbounded"/>
2997         </xs:sequence>
2998         <xs:attribute name="ID" type="xs:ID"/>
2999       </xs:restriction>
3000     </xs:complexContent>
3001   </xs:complexType>
3002
3003   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3004
3005   <xs:complexType name="AuthnMethodType">
3006     <xs:complexContent>
3007       <xs:restriction base="ac:AuthnMethodBaseType">
3008         <xs:sequence>
3009           <xs:element ref="AuthnMechanism"/>
3010           <xs:element ref="Authenticator"/>
3011           <xs:element ref="ac:AuthenticatorTransportProtocol"
3012 minOccurs="0"/>
3013           <xs:element ref="ac:Extension" minOccurs="0"
3014 maxOccurs="unbounded"/>
3015         </xs:sequence>
3016       </xs:restriction>
3017     </xs:complexContent>
```

```

3018     </xs:complexType>
3019
3020     <xs:element name="AuthnMechanism"
3021     type="PasswordAuthnMechanismType"/>
3022
3023     <xs:complexType name="PasswordAuthnMechanismType">
3024         <xs:complexContent>
3025             <xs:restriction
3026             base="ac:PrincipalAuthenticationMechanismType">
3027                 <xs:sequence>
3028                     <xs:choice>
3029                         <xs:element ref="ac:RestrictedPassword"/>
3030                     </xs:choice>
3031                 </xs:sequence>
3032                 <xs:attribute name="preauth" type="xs:integer"
3033                 use="optional"/>
3034             </xs:restriction>
3035         </xs:complexContent>
3036     </xs:complexType>
3037
3038     <xs:element name="Authenticator" type="AuthenticatorType"/>
3039
3040     <xs:complexType name="AuthenticatorType">
3041         <xs:complexContent>
3042             <xs:restriction base="ac:AuthenticatorBaseType">
3043                 <xs:choice>
3044                     <xs:element ref="DigSig"/>
3045                 </xs:choice>
3046             </xs:restriction>
3047         </xs:complexContent>
3048     </xs:complexType>
3049
3050     <xs:element name="DigSig" type="DigSigType"/>
3051
3052     <xs:complexType name="DigSigType">
3053         <xs:complexContent>
3054             <xs:restriction base="ac:PublicKeyType">
3055                 <xs:attribute name="keyValidation"
3056                 fixed="urn:ietf:rfc:3075"/>
3057             </xs:restriction>
3058         </xs:complexContent>
3059     </xs:complexType>
3060
3061 </xs:schema>

```

3062 **3.4.15 Smartcard**

3063 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard

3064 The Smartcard class is identified when a Principal authenticates to an authentication authority using a
3065 smartcard.

```

3066 <?xml version="1.0" encoding="UTF-8"?>
3067
3068 <xs:schema
3069 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
3070 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3071 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3072 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
3073 finalDefault="extension">
3074

```

```

3075     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3076     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3077
3078     <xs:annotation>
3079       <xs:documentation>
3080         urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
3081       </xs:documentation>
3082     </xs:annotation>
3083
3084     <xs:complexType name="AuthnContextDeclaration">
3085       <xs:complexContent>
3086         <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3087           <xs:sequence>
3088             <xs:element ref="ac:Identification" minOccurs="0"/>
3089             <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3090             <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3091             <xs:element ref="AuthnMethod"/>
3092             <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3093             <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3094               maxOccurs="unbounded"/>
3095             <xs:element ref="ac:Extension" minOccurs="0"
3096               maxOccurs="unbounded"/>
3097           </xs:sequence>
3098           <xs:attribute name="ID" type="xs:ID"/>
3099         </xs:restriction>
3100       </xs:complexContent>
3101     </xs:complexType>
3102
3103     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3104
3105     <xs:complexType name="AuthnMethodType">
3106       <xs:complexContent>
3107         <xs:restriction base="ac:AuthnMethodBaseType">
3108           <xs:sequence>
3109             <xs:element ref="AuthnMechanism"/>
3110             <xs:element ref="ac:Authenticator"/>
3111             <xs:element ref="ac:AuthenticatorTransportProtocol"
3112               minOccurs="0"/>
3113             <xs:element ref="ac:Extension" minOccurs="0"
3114               maxOccurs="unbounded"/>
3115           </xs:sequence>
3116         </xs:restriction>
3117       </xs:complexContent>
3118     </xs:complexType>
3119
3120     <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>
3121
3122     <xs:complexType name="SmartcardAuthnMechanismType">
3123       <xs:complexContent>
3124         <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
3125           <xs:sequence>
3126             <xs:choice>
3127               <xs:element ref="ac:Smartcard"/>
3128             </xs:choice>
3129           </xs:sequence>
3130         </xs:restriction>
3131       </xs:complexContent>
3132     </xs:complexType>
3133
3134 </xs:schema>

```

3135 **3.4.16 SmartcardPKI**

3136 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

3137 The SmartcardPKI class is identified when a Principal authenticates to an authentication authority through

3138 a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN.

```
3139 <?xml version="1.0" encoding="UTF-8"?>
3140
3141 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
3142   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3143   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3144   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
3145   finalDefault="extension">
3146
3147   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac" schemaLocation="sstc-saml-
3148   schema-authn-context-1.0.xsd"/>
3149
3150   <xs:annotation>
3151     <xs:documentation>
3152       urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
3153     </xs:documentation>
3154   </xs:annotation>
3155
3156   <xs:complexType name="AuthnContextDeclaration">
3157     <xs:complexContent>
3158       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3159         <xs:sequence>
3160           <xs:element ref="ac:Identification" minOccurs="0"/>
3161           <xs:element ref="TechnicalProtection"/>
3162           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3163           <xs:element ref="AuthnMethod"/>
3164           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3165           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3166             maxOccurs="unbounded"/>
3167           <xs:element ref="ac:Extension" minOccurs="0"
3168             maxOccurs="unbounded"/>
3169         </xs:sequence>
3170         <xs:attribute name="ID" type="xs:ID"/>
3171       </xs:restriction>
3172     </xs:complexContent>
3173   </xs:complexType>
3174
3175   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3176
3177   <xs:complexType name="AuthnMethodType">
3178     <xs:complexContent>
3179       <xs:restriction base="ac:AuthnMethodBaseType">
3180         <xs:sequence>
3181           <xs:element ref="AuthnMechanism"/>
3182           <xs:element ref="Authenticator"/>
3183           <xs:element ref="ac:AuthenticatorTransportProtocol"
3184             minOccurs="0"/>
3185           <xs:element ref="ac:Extension" minOccurs="0"
3186             maxOccurs="unbounded"/>
3187         </xs:sequence>
3188       </xs:restriction>
3189     </xs:complexContent>
3190   </xs:complexType>
3191
3192   <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
3193
3194   <xs:complexType name="TechnicalProtectionType">
3195     <xs:complexContent>
3196       <xs:restriction base="ac:TechnicalProtectionBaseType">
3197         <xs:sequence>
3198           <xs:choice>
3199             <xs:element ref="PrivateKeyProtection"/>
3200             <xs:element ref="ac:SecretKeyProtection" minOccurs="0"/>
3201             <xs:element ref="ac:Extension" minOccurs="0"
3202               maxOccurs="unbounded"/>
3203           </xs:choice>
3204         </xs:sequence>
```

```

3205     </xs:restriction>
3206   </xs:complexContent>
3207 </xs:complexType>
3208
3209 <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>
3210
3211 <xs:complexType name="SmartcardAuthnMechanismType">
3212   <xs:complexContent>
3213     <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
3214       <xs:sequence>
3215         <xs:element ref="ac:ActivationPin"/>
3216         <xs:element ref="ac:Smartcard"/>
3217         <xs:element ref="ac:Extension" minOccurs="0" maxOccurs="unbounded"/>
3218       </xs:sequence>
3219     </xs:restriction>
3220   </xs:complexContent>
3221 </xs:complexType>
3222
3223 <xs:element name="Authenticator" type="SmartCardPKIAuthenticatorType"/>
3224
3225 <xs:complexType name="SmartCardPKIAuthenticatorType">
3226   <xs:complexContent>
3227     <xs:restriction base="ac:AuthenticatorBaseType">
3228       <xs:choice>
3229         <xs:element ref="ac:AsymmetricDecryption"/>
3230         <xs:element ref="ac:AsymmetricKeyAgreement"/>
3231         <xs:element ref="ac:DigSig"/>
3232       </xs:choice>
3233     </xs:restriction>
3234   </xs:complexContent>
3235 </xs:complexType>
3236
3237 <xs:element name="PrivateKeyProtection" type="PrivateKeyProtectionType"/>
3238
3239 <xs:complexType name="PrivateKeyProtectionType">
3240   <xs:complexContent>
3241     <xs:restriction base="ac:PrivateKeyProtectionType">
3242       <xs:sequence>
3243         <xs:element ref="KeyActivation"/>
3244         <xs:element ref="KeyStorage"/>
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="KeyActivation" type="KeyActivationType"/>
3252
3253 <xs:complexType name="KeyActivationType">
3254   <xs:complexContent>
3255     <xs:restriction base="ac:KeyActivationType">
3256       <xs:choice>
3257         <xs:element ref="ac:ActivationPin"/>
3258       </xs:choice>
3259     </xs:restriction>
3260   </xs:complexContent>
3261 </xs:complexType>
3262
3263 <xs:element name="KeyStorage" type="KeyStorageType"/>
3264
3265 <xs:complexType name="KeyStorageType">
3266   <xs:complexContent>
3267     <xs:restriction base="ac:KeyStorageType">
3268       <xs:attribute name="medium" use="required">
3269         <xs:simpleType>
3270           <xs:restriction base="xs:NMTOKEN">
3271             <xs:enumeration value="smartcard"/>

```

```
3272         </xs:restriction>
3273     </xs:simpleType>
3274     </xs:attribute>
3275 </xs:restriction>
3276 </xs:complexContent>
3277 </xs:complexType>
3278
3279 </xs:schema>
```

3280 3.4.17 SoftwarePKI

3281 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI

3282 The Software-PKI class is identified when a Principal uses an X.509 certificate stored in software to
3283 authenticate to the authentication authority.

```
3284 <?xml version="1.0" encoding="UTF-8"?>
3285
3286 <xs:schema
3287 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3288 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3289 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3290 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3291 finalDefault="extension">
3292
3293     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3294 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3295
3296     <xs:annotation>
3297         <xs:documentation>
3298             urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
3299         </xs:documentation>
3300     </xs:annotation>
3301
3302     <xs:complexType name="AuthnContextDeclaration">
3303         <xs:complexContent>
3304             <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3305                 <xs:sequence>
3306                     <xs:element ref="ac:Identification" minOccurs="0"/>
3307                     <xs:element ref="TechnicalProtection"/>
3308                     <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3309                     <xs:element ref="AuthnMethod"/>
3310                     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3311                     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3312 maxOccurs="unbounded"/>
3313                     <xs:element ref="ac:Extension" minOccurs="0"
3314 maxOccurs="unbounded"/>
3315                 </xs:sequence>
3316                 <xs:attribute name="ID" type="xs:ID"/>
3317             </xs:restriction>
3318         </xs:complexContent>
3319     </xs:complexType>
3320
3321     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3322
3323     <xs:complexType name="AuthnMethodType">
3324         <xs:complexContent>
3325             <xs:restriction base="ac:AuthnMethodBaseType">
3326                 <xs:sequence>
3327                     <xs:element ref="AuthnMechanism"/>
3328                     <xs:element ref="Authenticator"/>
3329                     <xs:element ref="ac:AuthenticatorTransportProtocol"
3330 minOccurs="0"/>
3331                     <xs:element ref="ac:Extension" minOccurs="0"
3332 maxOccurs="unbounded"/>
3333                 </xs:sequence>
```

```

3334     </xs:restriction>
3335     </xs:complexContent>
3336 </xs:complexType>
3337
3338 <xs:element name="TechnicalProtection" type="TechnicalProtectionType"/>
3339
3340 <xs:complexType name="TechnicalProtectionType">
3341   <xs:complexContent>
3342     <xs:restriction base="ac:TechnicalProtectionBaseType">
3343       <xs:sequence>
3344         <xs:choice>
3345           <xs:element ref="PrivateKeyProtection"/>
3346           <xs:element ref="ac:SecretKeyProtection" minOccurs="0"/>
3347           <xs:element ref="ac:Extension" minOccurs="0"
3348             maxOccurs="unbounded"/>
3349         </xs:choice>
3350       </xs:sequence>
3351     </xs:restriction>
3352   </xs:complexContent>
3353 </xs:complexType>
3354
3355 <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>
3356
3357 <xs:complexType name="SmartcardAuthnMechanismType">
3358   <xs:complexContent>
3359     <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
3360       <xs:sequence>
3361         <xs:element ref="ac:ActivationPin"/>
3362         <xs:element ref="ac:Extension" minOccurs="0"
3363           maxOccurs="unbounded"/>
3364       </xs:sequence>
3365     </xs:restriction>
3366   </xs:complexContent>
3367 </xs:complexType>
3368
3369 <xs:element name="Authenticator" type="SmartCardPKIAuthenticatorType"/>
3370
3371 <xs:complexType name="SmartCardPKIAuthenticatorType">
3372   <xs:complexContent>
3373     <xs:restriction base="ac:AuthenticatorBaseType">
3374       <xs:choice>
3375         <xs:element ref="ac:AsymmetricDecryption"/>
3376         <xs:element ref="ac:AsymmetricKeyAgreement"/>
3377         <xs:element ref="ac:DigSig"/>
3378       </xs:choice>
3379     </xs:restriction>
3380   </xs:complexContent>
3381 </xs:complexType>
3382
3383 <xs:element name="PrivateKeyProtection"
3384 type="PrivateKeyProtectionType"/>
3385
3386 <xs:complexType name="PrivateKeyProtectionType">
3387   <xs:complexContent>
3388     <xs:restriction base="ac:PrivateKeyProtectionType">
3389       <xs:sequence>
3390         <xs:element ref="KeyActivation"/>
3391         <xs:element ref="KeyStorage"/>
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="KeyActivation" type="KeyActivationType"/>
3400

```

```

3401 <xs:complexType name="KeyActivationType">
3402   <xs:complexContent>
3403     <xs:restriction base="ac:KeyActivationType">
3404       <xs:choice>
3405         <xs:element ref="ac:ActivationPin"/>
3406       </xs:choice>
3407     </xs:restriction>
3408   </xs:complexContent>
3409 </xs:complexType>
3410
3411 <xs:element name="KeyStorage" type="KeyStorageType"/>
3412
3413 <xs:complexType name="KeyStorageType">
3414   <xs:complexContent>
3415     <xs:restriction base="ac:KeyStorageType">
3416       <xs:attribute name="medium" use="required">
3417         <xs:simpleType>
3418           <xs:restriction base="xs:NMTOKEN">
3419             <xs:enumeration value="memory"/>
3420           </xs:restriction>
3421         </xs:simpleType>
3422       </xs:attribute>
3423     </xs:restriction>
3424   </xs:complexContent>
3425 </xs:complexType>
3426
3427 </xs:schema>

```

3428 3.4.18 Telephony

3429 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony

3430 This class is used to indicate that the Principal authenticated via the provision of a fixed-line telephone
3431 number, transported via a telephony protocol such as ADSL.

```

3432 <?xml version="1.0" encoding="UTF-8"?>
3433
3434 <xs:schema
3435 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3436 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3437 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3438 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3439 finalDefault="extension">
3440
3441   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3442 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3443
3444   <xs:annotation>
3445     <xs:documentation>
3446       urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
3447     </xs:documentation>
3448   </xs:annotation>
3449
3450   <xs:complexType name="AuthnContextDeclaration">
3451     <xs:complexContent>
3452       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3453         <xs:sequence>
3454           <xs:element ref="ac:Identification" minOccurs="0"/>
3455           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3456           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3457           <xs:element ref="AuthnMethod"/>
3458           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3459           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3460             maxOccurs="unbounded"/>
3461           <xs:element ref="ac:Extension" minOccurs="0"
3462             maxOccurs="unbounded"/>

```

```

3463         </xs:sequence>
3464         <xs:attribute name="ID" type="xs:ID"/>
3465     </xs:restriction>
3466 </xs:complexContent>
3467 </xs:complexType>
3468
3469 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3470
3471 <xs:complexType name="AuthnMethodType">
3472     <xs:complexContent>
3473         <xs:restriction base="ac:AuthnMethodBaseType">
3474             <xs:sequence>
3475                 <xs:element ref="ac:PrincipalAuthenticationMechanism"
3476 minOccurs="0"/>
3477                 <xs:element ref="Authenticator"/>
3478                 <xs:element ref="AuthenticatorTransportProtocol"/>
3479                 <xs:element ref="ac:Extension" minOccurs="0"
3480 maxOccurs="unbounded"/>
3481             </xs:sequence>
3482         </xs:restriction>
3483     </xs:complexContent>
3484 </xs:complexType>
3485
3486 <xs:element name="Authenticator" type="AuthenticatorType"/>
3487
3488 <xs:complexType name="AuthenticatorType">
3489     <xs:complexContent>
3490         <xs:restriction base="ac:AuthenticatorBaseType">
3491             <xs:choice>
3492                 <xs:element ref="ac:SubscriberLineNumber"/>
3493             </xs:choice>
3494         </xs:restriction>
3495     </xs:complexContent>
3496 </xs:complexType>
3497
3498 <xs:element name="AuthenticatorTransportProtocol"
3499 type="TransportType"/>
3500
3501 <xs:complexType name="TransportType">
3502     <xs:complexContent>
3503         <xs:restriction base="ac:AuthenticatorTransportProtocolType">
3504             <xs:choice>
3505                 <xs:element ref="ac:PSTN"/>
3506                 <xs:element ref="ac:ISDN"/>
3507                 <xs:element ref="ac:ADSL"/>
3508             </xs:choice>
3509         </xs:restriction>
3510     </xs:complexContent>
3511 </xs:complexType>
3512
3513 </xs:schema>

```

3514 3.4.19 Telephony ("Nomadic")

3515 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony

3516 Indicates that the Principal is "roaming" (perhaps using a phone card) and authenticates via the means of
3517 the line number, a user suffix, and a password element.

```

3518 <?xml version="1.0" encoding="UTF-8"?>
3519
3520 <xs:schema
3521 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3522 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3523 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3524 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"

```

```

3525     finalDefault="extension">
3526
3527     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3528     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3529
3530     <xs:annotation>
3531     <xs:documentation>
3532     urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
3533     </xs:documentation>
3534     </xs:annotation>
3535
3536     <xs:complexType name="AuthnContextDeclaration">
3537     <xs:complexContent>
3538     <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3539     <xs:sequence>
3540     <xs:element ref="ac:Identification" minOccurs="0"/>
3541     <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3542     <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3543     <xs:element ref="AuthnMethod"/>
3544     <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3545     <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3546     maxOccurs="unbounded"/>
3547     <xs:element ref="ac:Extension" minOccurs="0"
3548     maxOccurs="unbounded"/>
3549     </xs:sequence>
3550     <xs:attribute name="ID" type="xs:ID"/>
3551     </xs:restriction>
3552     </xs:complexContent>
3553     </xs:complexType>
3554
3555     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3556
3557     <xs:complexType name="AuthnMethodType">
3558     <xs:complexContent>
3559     <xs:restriction base="ac:AuthnMethodBaseType">
3560     <xs:sequence>
3561     <xs:element ref="ac:PrincipalAuthenticationMechanism"
3562     minOccurs="0"/>
3563     <xs:element ref="Authenticator"/>
3564     <xs:element ref="AuthenticatorTransportProtocol"/>
3565     <xs:element ref="ac:Extension" minOccurs="0"
3566     maxOccurs="unbounded"/>
3567     </xs:sequence>
3568     </xs:restriction>
3569     </xs:complexContent>
3570     </xs:complexType>
3571
3572     <xs:element name="Authenticator" type="AuthenticatorType"/>
3573
3574     <xs:complexType name="AuthenticatorType">
3575     <xs:complexContent>
3576     <xs:restriction base="ac:AuthenticatorBaseType">
3577     <xs:sequence>
3578     <xs:element ref="ac:SubscriberLineNumber"/>
3579     <xs:element ref="ac:UserSuffix"/>
3580     <xs:element ref="ac:Password"/>
3581     </xs:sequence>
3582     </xs:restriction>
3583     </xs:complexContent>
3584     </xs:complexType>
3585
3586     <xs:element name="AuthenticatorTransportProtocol"
3587     type="TransportType"/>
3588
3589     <xs:complexType name="TransportType">
3590     <xs:complexContent>
3591     <xs:restriction base="ac:AuthenticatorTransportProtocolType">

```

```

3592     <xs:choice>
3593         <xs:element ref="ac:PSTN"/>
3594         <xs:element ref="ac:ISDN"/>
3595         <xs:element ref="ac:ADSL"/>
3596     </xs:choice>
3597 </xs:restriction>
3598 </xs:complexContent>
3599 </xs:complexType>
3600
3601 </xs:schema>

```

3602 3.4.20 Telephony (Personalized)

3603 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony

3604 This class is used to indicate that the Principal authenticated via the provision of a fixed-line telephone
3605 number and a user suffix, transported via a telephony protocol such as ADSL.

```

3606 <?xml version="1.0" encoding="UTF-8"?>
3607
3608 <xs:schema
3609   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelep
3610 hony"
3611   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3612   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3613   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
3614   finalDefault="extension">
3615
3616   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3617   schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3618
3619   <xs:annotation>
3620     <xs:documentation>
3621       urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony
3622     </xs:documentation>
3623   </xs:annotation>
3624
3625   <xs:complexType name="AuthnContextDeclaration">
3626     <xs:complexContent>
3627       <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3628         <xs:sequence>
3629           <xs:element ref="ac:Identification" minOccurs="0"/>
3630           <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3631           <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3632           <xs:element ref="AuthnMethod"/>
3633           <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3634           <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3635             maxOccurs="unbounded"/>
3636           <xs:element ref="ac:Extension" minOccurs="0"
3637             maxOccurs="unbounded"/>
3638         </xs:sequence>
3639         <xs:attribute name="ID" type="xs:ID"/>
3640       </xs:restriction>
3641     </xs:complexContent>
3642   </xs:complexType>
3643
3644   <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3645
3646   <xs:complexType name="AuthnMethodType">
3647     <xs:complexContent>
3648       <xs:restriction base="ac:AuthnMethodBaseType">
3649         <xs:sequence>
3650           <xs:element ref="ac:PrincipalAuthenticationMechanism"
3651             minOccurs="0"/>
3652           <xs:element ref="Authenticator"/>
3653           <xs:element ref="AuthenticatorTransportProtocol"/>

```

```

3654         <xs:element ref="ac:Extension" minOccurs="0"
3655             maxOccurs="unbounded"/>
3656     </xs:sequence>
3657 </xs:restriction>
3658 </xs:complexContent>
3659 </xs:complexType>
3660
3661 <xs:element name="Authenticator" type="AuthenticatorType"/>
3662
3663 <xs:complexType name="AuthenticatorType">
3664     <xs:complexContent>
3665         <xs:restriction base="ac:AuthenticatorBaseType">
3666             <xs:sequence>
3667                 <xs:element ref="ac:SubscriberLineNumber"/>
3668                 <xs:element ref="ac:UserSuffix"/>
3669             </xs:sequence>
3670         </xs:restriction>
3671     </xs:complexContent>
3672 </xs:complexType>
3673
3674 <xs:element name="AuthenticatorTransportProtocol"
3675     type="TransportType"/>
3676
3677 <xs:complexType name="TransportType">
3678     <xs:complexContent>
3679         <xs:restriction base="ac:AuthenticatorTransportProtocolType">
3680             <xs:choice>
3681                 <xs:element ref="ac:PSTN"/>
3682                 <xs:element ref="ac:ISDN"/>
3683                 <xs:element ref="ac:ADSL"/>
3684             </xs:choice>
3685         </xs:restriction>
3686     </xs:complexContent>
3687 </xs:complexType>
3688
3689 </xs:schema>

```

3690 3.4.21 Telephony (Authenticated)

3691 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony

3692 Indicates that the Principal authenticated via the means of the line number, a user suffix, and a password
3693 element.

```

3694 <?xml version="1.0" encoding="UTF-8"?>
3695
3696 <xs:schema
3697     targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3698     xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3699     xmlns:xs="http://www.w3.org/2001/XMLSchema"
3700     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3701     finalDefault="extension">
3702
3703     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3704         schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3705
3706     <xs:annotation>
3707         <xs:documentation>
3708             urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
3709         </xs:documentation>
3710     </xs:annotation>
3711
3712     <xs:complexType name="AuthnContextDeclaration">
3713         <xs:complexContent>
3714             <xs:restriction base="ac:AuthnContextDeclarationBaseType">

```

```

3716     <xs:sequence>
3717         <xs:element ref="ac:Identification" minOccurs="0"/>
3718         <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3719         <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
3720         <xs:element ref="AuthnMethod"/>
3721         <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3722         <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
3723             maxOccurs="unbounded"/>
3724         <xs:element ref="ac:Extension" minOccurs="0"
3725             maxOccurs="unbounded"/>
3726     </xs:sequence>
3727     <xs:attribute name="ID" type="xs:ID"/>
3728 </xs:restriction>
3729 </xs:complexContent>
3730 </xs:complexType>
3731
3732 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3733
3734 <xs:complexType name="AuthnMethodType">
3735     <xs:complexContent>
3736         <xs:restriction base="ac:AuthnMethodBaseType">
3737             <xs:sequence>
3738                 <xs:element ref="ac:PrincipalAuthenticationMechanism"
3739 minOccurs="0"/>
3740                 <xs:element ref="Authenticator"/>
3741                 <xs:element ref="AuthenticatorTransportProtocol"/>
3742                 <xs:element ref="ac:Extension" minOccurs="0"
3743                     maxOccurs="unbounded"/>
3744             </xs:sequence>
3745         </xs:restriction>
3746     </xs:complexContent>
3747 </xs:complexType>
3748
3749 <xs:element name="Authenticator" type="AuthenticatorType"/>
3750
3751 <xs:complexType name="AuthenticatorType">
3752     <xs:complexContent>
3753         <xs:restriction base="ac:AuthenticatorBaseType">
3754             <xs:sequence>
3755                 <xs:element ref="ac:SubscriberLineNumber"/>
3756                 <xs:element ref="ac:UserSuffix"/>
3757                 <xs:element ref="ac:Password"/>
3758             </xs:sequence>
3759         </xs:restriction>
3760     </xs:complexContent>
3761 </xs:complexType>
3762
3763 <xs:element name="AuthenticatorTransportProtocol"
3764 type="TransportType"/>
3765
3766 <xs:complexType name="TransportType">
3767     <xs:complexContent>
3768         <xs:restriction base="ac:AuthenticatorTransportProtocolType">
3769             <xs:choice>
3770                 <xs:element ref="ac:PSTN"/>
3771                 <xs:element ref="ac:ISDN"/>
3772                 <xs:element ref="ac:ADSL"/>
3773             </xs:choice>
3774         </xs:restriction>
3775     </xs:complexContent>
3776 </xs:complexType>
3777
3778 </xs:schema>

```

3779 3.4.22 Secure Remote Password

3780 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword

3781 The Secure Remote Password class is indicated when the authentication was performed by means of
3782 Secure Remote Password as specified in [RFC2945].

```
3783 <?xml version="1.0" encoding="UTF-8"?>
3784
3785 <xs:schema
3786 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRem
3787 otePassword"
3788 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3789 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3790 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassw
3791 ord"
3792 finalDefault="extension">
3793
3794 <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3795 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3796
3797 <xs:annotation>
3798 <xs:documentation>
3799 urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
3800 </xs:documentation>
3801 </xs:annotation>
3802
3803 <xs:complexType name="AuthnContextDeclaration">
3804 <xs:complexContent>
3805 <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3806 <xs:sequence>
3807 <xs:element ref="ac:Identification" minOccurs="0"/>
3808 <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3809 <xs:element ref="ac:OperationalProtection"
3810 minOccurs="0"/>
3811 <xs:element ref="AuthnMethod"/>
3812 <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3813 <xs:element ref="ac:AuthenticatingAuthority"
3814 minOccurs="0"
3815 maxOccurs="unbounded"/>
3816 <xs:element ref="ac:Extension" minOccurs="0"
3817 maxOccurs="unbounded"/>
3818 </xs:sequence>
3819 <xs:attribute name="ID" type="xs:ID"/>
3820 </xs:restriction>
3821 </xs:complexContent>
3822 </xs:complexType>
3823
3824 <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3825
3826 <xs:complexType name="AuthnMethodType">
3827 <xs:complexContent>
3828 <xs:restriction base="ac:AuthnMethodBaseType">
3829 <xs:sequence>
3830 <xs:element ref="PrincipalAuthenticationMechanism"/>
3831 <xs:element ref="Authenticator"/>
3832 <xs:element ref="ac:AuthenticatorTransportProtocol"
3833 minOccurs="0"/>
3834 <xs:element ref="ac:Extension" minOccurs="0"
3835 maxOccurs="unbounded"/>
3836 </xs:sequence>
```

```

3837     </xs:restriction>
3838     </xs:complexContent>
3839   </xs:complexType>
3840
3841   <xs:element name="PrincipalAuthenticationMechanism"
3842     type="PasswordAuthnMechanismType"/>
3843
3844   <xs:complexType name="PasswordAuthnMechanismType">
3845     <xs:complexContent>
3846       <xs:restriction
3847         base="ac:PrincipalAuthenticationMechanismType">
3848         <xs:sequence>
3849           <xs:choice>
3850             <xs:element ref="ac:RestrictedPassword"/>
3851           </xs:choice>
3852         </xs:sequence>
3853       </xs:restriction>
3854     </xs:complexContent>
3855   </xs:complexType>
3856
3857   <xs:element name="Authenticator" type="SharedSecretType"/>
3858
3859   <xs:complexType name="SharedSecretType">
3860     <xs:complexContent>
3861       <xs:restriction base="ac:AuthenticatorBaseType">
3862         <xs:choice>
3863           <xs:element ref="SharedSecretChallengeResponse"/>
3864         </xs:choice>
3865       </xs:restriction>
3866     </xs:complexContent>
3867   </xs:complexType>
3868
3869   <xs:element name="SharedSecretChallengeResponse"
3870     type="ChallengeResponseType"/>
3871
3872   <xs:complexType name="ChallengeResponseType">
3873     <xs:complexContent>
3874       <xs:restriction base="ac:SharedSecretChallengeResponseType">
3875         <xs:attribute name="method" fixed="urn:ietf:rfc:2945"/>
3876       </xs:restriction>
3877     </xs:complexContent>
3878   </xs:complexType>
3879
3880 </xs:schema>

```

3881 **3.4.23 SSL/TLS Certificate-Based Client Authentication**

3882 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClnt

3883 This class indicates that the Principal authenticated by means of a client certificate, secured with the
3884 SSL/TLS transport.

```

3885 <?xml version="1.0" encoding="UTF-8"?>
3886
3887 <xs:schema
3888   targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClnt"
3889   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
3890   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3891   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClnt"
3892   finalDefault="extension">
3893

```

```

3894     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
3895     schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
3896
3897     <xs:annotation>
3898       <xs:documentation>
3899         urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
3900       </xs:documentation>
3901     </xs:annotation>
3902
3903     <xs:complexType name="AuthnContextDeclaration">
3904       <xs:complexContent>
3905         <xs:restriction base="ac:AuthnContextDeclarationBaseType">
3906           <xs:sequence>
3907             <xs:element ref="ac:Identification" minOccurs="0"/>
3908             <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
3909             <xs:element ref="ac:OperationalProtection"
3910             minOccurs="0"/>
3911             <xs:element ref="AuthnMethod"/>
3912             <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
3913             <xs:element ref="ac:AuthenticatingAuthority"
3914             minOccurs="0"
3915             maxOccurs="unbounded"/>
3916             <xs:element ref="ac:Extension" minOccurs="0"
3917             maxOccurs="unbounded"/>
3918           </xs:sequence>
3919           <xs:attribute name="ID" type="xs:ID"/>
3920         </xs:restriction>
3921       </xs:complexContent>
3922     </xs:complexType>
3923
3924     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
3925
3926     <xs:complexType name="AuthnMethodType">
3927       <xs:complexContent>
3928         <xs:restriction base="ac:AuthnMethodBaseType">
3929           <xs:sequence>
3930             <xs:element ref="AuthnMechanism"/>
3931             <xs:element ref="Authenticator"/>
3932             <xs:element ref="AuthenticatorTransportProtocol"
3933             minOccurs="0"/>
3934             <xs:element ref="ac:Extension" minOccurs="0"
3935             maxOccurs="unbounded"/>
3936           </xs:sequence>
3937         </xs:restriction>
3938       </xs:complexContent>
3939     </xs:complexType>
3940
3941     <xs:element name="AuthnMechanism"
3942     type="PasswordAuthnMechanismType"/>
3943
3944     <xs:complexType name="PasswordAuthnMechanismType">
3945       <xs:complexContent>
3946         <xs:restriction
3947         base="ac:PrincipalAuthenticationMechanismType">
3948           <xs:sequence>
3949             <xs:choice>
3950               <xs:element ref="ac:RestrictedPassword"/>
3951             </xs:choice>
3952           </xs:sequence>
3953           <xs:attribute name="preauth" type="xs:integer"
3954           use="optional"/>

```

```

3955     </xs:restriction>
3956     </xs:complexContent>
3957 </xs:complexType>
3958
3959 <xs:element name="Authenticator" type="AuthenticatorType"/>
3960
3961 <xs:complexType name="AuthenticatorType">
3962     <xs:complexContent>
3963         <xs:restriction base="ac:AuthenticatorBaseType">
3964             <xs:choice>
3965                 <xs:element ref="DigSig"/>
3966             </xs:choice>
3967         </xs:restriction>
3968     </xs:complexContent>
3969 </xs:complexType>
3970
3971 <xs:element name="DigSig" type="DigSigType"/>
3972
3973 <xs:complexType name="DigSigType">
3974     <xs:complexContent>
3975         <xs:restriction base="ac:PublicKeyType">
3976             <xs:attribute name="keyValidation"
3977 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
3978         </xs:restriction>
3979     </xs:complexContent>
3980 </xs:complexType>
3981
3982 <xs:element name="AuthenticatorTransportProtocol"
3983 type="ProtectedProtocolType"/>
3984
3985 <xs:complexType name="ProtectedProtocolType">
3986     <xs:complexContent>
3987         <xs:restriction
3988 base="ac:AuthenticatorTransportProtocolType">
3989             <xs:choice>
3990                 <xs:element ref="ac:SSL"/>
3991                 <xs:element ref="ac:WTLS"/>
3992             </xs:choice>
3993         </xs:restriction>
3994     </xs:complexContent>
3995 </xs:complexType>
3996
3997 </xs:schema>

```

3998 **3.4.24 TimeSyncToken**

3999 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken

4000 The TimeSyncToken class is identified when a Principal authenticates through a time synchronization
4001 token.

```

4002 <?xml version="1.0" encoding="UTF-8"?>
4003
4004 <xs:schema
4005 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
4006 xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
4007 xmlns:xs="http://www.w3.org/2001/XMLSchema"
4008 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
4009 finalDefault="extension">
4010
4011     <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
4012 schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

```

```

4013
4014     <xs:annotation>
4015       <xs:documentation>
4016         urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
4017       </xs:documentation>
4018     </xs:annotation>
4019
4020     <xs:complexType name="AuthnContextDeclaration">
4021       <xs:complexContent>
4022         <xs:restriction base="ac:AuthnContextDeclarationBaseType">
4023           <xs:sequence>
4024             <xs:element ref="ac:Identification" minOccurs="0"/>
4025             <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
4026             <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
4027             <xs:element ref="AuthnMethod"/>
4028             <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
4029             <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
4030               maxOccurs="unbounded"/>
4031             <xs:element ref="ac:Extension" minOccurs="0"
4032               maxOccurs="unbounded"/>
4033           </xs:sequence>
4034           <xs:attribute name="ID" type="xs:ID"/>
4035         </xs:restriction>
4036       </xs:complexContent>
4037     </xs:complexType>
4038
4039     <xs:element name="AuthnMethod" type="AuthnMethodType"/>
4040
4041     <xs:complexType name="AuthnMethodType">
4042       <xs:complexContent>
4043         <xs:restriction base="ac:AuthnMethodBaseType">
4044           <xs:sequence>
4045             <xs:element ref="PrincipalAuthenticationMechanism"
4046               minOccurs="0"/>
4047             <xs:element ref="ac:Authenticator"/>
4048             <xs:element ref="ac:AuthenticatorTransportProtocol"
4049               minOccurs="0"/>
4050             <xs:element ref="ac:Extension" minOccurs="0"
4051               maxOccurs="unbounded"/>
4052           </xs:sequence>
4053         </xs:restriction>
4054       </xs:complexContent>
4055     </xs:complexType>
4056
4057     <xs:element name="PrincipalAuthenticationMechanism"
4058       type="TimeSyncMechType"/>
4059
4060     <xs:complexType name="TimeSyncMechType">
4061       <xs:complexContent>
4062         <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
4063           <xs:choice>
4064             <xs:element ref="Token"/>
4065           </xs:choice>
4066         </xs:restriction>
4067       </xs:complexContent>
4068     </xs:complexType>
4069
4070     <xs:element name="Token" type="TokenType"/>
4071
4072     <xs:complexType name="TokenType">
4073       <xs:complexContent>
4074         <xs:restriction base="ac:TokenType">
4075           <xs:sequence>
4076             <xs:element ref="TimeSyncToken"/>
4077             <xs:element ref="ac:Extension" minOccurs="0"
4078               maxOccurs="unbounded"/>
4079           </xs:sequence>

```

```

4080     </xs:restriction>
4081     </xs:complexContent>
4082 </xs:complexType>
4083
4084 <xs:element name="TimeSyncToken" type="TimeSyncTokenType"/>
4085
4086 <xs:complexType name="TimeSyncTokenType">
4087   <xs:complexContent>
4088     <xs:restriction base="ac:TimeSyncTokenType">
4089
4090       <xs:attribute name="DeviceType" use="required">
4091         <xs:simpleType>
4092           <xs:restriction base="xs:NMTOKEN">
4093             <xs:enumeration value="hardware"/>
4094           </xs:restriction>
4095         </xs:simpleType>
4096       </xs:attribute>
4097
4098       <xs:attribute name="SeedLength" use="required">
4099         <xs:simpleType>
4100           <xs:restriction base="xs:integer">
4101             <xs:minInclusive value="64"/>
4102           </xs:restriction>
4103         </xs:simpleType>
4104       </xs:attribute>
4105
4106       <xs:attribute name="DeviceInHand" use="required">
4107         <xs:simpleType>
4108           <xs:restriction base="xs:NMTOKEN">
4109             <xs:enumeration value="true"/>
4110           </xs:restriction>
4111         </xs:simpleType>
4112       </xs:attribute>
4113     </xs:restriction>
4114   </xs:complexContent>
4115 </xs:complexType>
4116
4117 </xs:schema>

```

4118 **3.4.25 Unspecified**

4119 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

4120 The Unspecified class indicates that the authentication was performed by unspecified means.

4121 4 References

- 4122 **[RFC1510]** TBS
- 4123 **[RFC2119]** eds. (March 1997). "Key words for use in RFCs to Indicate Requirement Levels,"
4124 RFC 2119., " <http://www.rfc-editor.org/rfc/rfc2119.txt>.
- 4125 **[RFC2945]** TBS
- 4126 **[SAMLCore]** Maler, E. et al., "Assertions and Protocol for the OASIS Security Assertion
4127 Markup Language (SAML) v2.0", Committee Draft.
- 4128 **[XMLSchema]** TBS
- 4129 [XMLSig] TBS

4130 **5 Acknowledgments**

4131 The following individuals were members of the committee during the development of this specification:

4132 TBS

6 Revision History

Rev	Date	By Whom	What
01	26 Jan 2004	John Kemp	Initial version
02	1 Feb 2004	John Kemp	Updated formatting, namespaces
03	18 Feb 2004	John Kemp	Added a note about authentication method, more formatting and namespace updates.
05	1 May 2004	John Kemp	Implemented SAML Authentication Methods as AC classes
06	25 Jun 2004	John Kemp	Developed schema-centric approach; revised text on creating new authentication context classes; Changed TimeSyncToken class to allow SeedLength >= 64
07	13 Jul 2004	Eve Maler	Cleanup to prepare for publication as a last-call working draft.

4135

7 Notices

4136 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
4137 might be claimed to pertain to the implementation or use of the technology described in this document or
4138 the extent to which any license under such rights might or might not be available; neither does it represent
4139 that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to
4140 rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made
4141 available for publication and any assurances of licenses to be made available, or the result of an attempt
4142 made to obtain a general license or permission for the use of such proprietary rights by implementors or
4143 users of this specification, can be obtained from the OASIS Executive Director.

4144 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or
4145 other proprietary rights which may cover technology that may be required to implement this specification.
4146 Please address the information to the OASIS Executive Director.

4147 **Copyright © OASIS Open 2004. All Rights Reserved.**

4148 This document and translations of it may be copied and furnished to others, and derivative works that
4149 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and
4150 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
4151 this paragraph are included on all such copies and derivative works. However, this document itself does
4152 not be modified in any way, such as by removing the copyright notice or references to OASIS, except as
4153 needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights
4154 defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it
4155 into languages other than English.

4156 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
4157 or assigns.

4158 This document and the information contained herein is provided on an "AS IS" basis and OASIS
4159 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
4160 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR
4161 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.