



1

---

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

5 **Committee Draft 03, 14 December 2004**

6 **Document identifier:**

7 sstc-saml-authn-context-2.0-cd-03

8 **Location:**

9 [http://www.oasis-open.org/committees/documents.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)

10 **Editors:**

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

15 **SAML V2.0 Contributors:**

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

45 Ron Monzillo, Sun Microsystems  
46 Greg Whitehead, Trustgenix

47 **Abstract:**

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

50 **Status:**

51 This is a **Committee Draft** approved by the Security Services Technical Committee on 14  
52 December 2004.

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

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

---

## 62 Table of Contents

63	1 Introduction.....	4
64	1.1 Authentication Context Concepts.....	4
65	1.2 Notation and Terminology.....	4
66	2 Authentication Context Declaration.....	6
67	2.1 Data Model.....	6
68	2.2 Extensibility.....	7
69	2.3 Processing Rules.....	7
70	2.4 Schema.....	7
71	3 Authentication Context Classes.....	23
72	3.1 Advantages of Authentication Context Classes.....	23
73	3.2 Processing Rules.....	23
74	3.3 Extensibility.....	24
75	3.4 Schemas.....	24
76	3.4.1 Internet Protocol.....	24
77	3.4.2 InternetProtocolPassword.....	26
78	3.4.3 Kerberos.....	27
79	3.4.4 MobileOneFactorUnregistered.....	29
80	3.4.5 MobileTwoFactorUnregistered.....	32
81	3.4.6 MobileOneFactorContract.....	36
82	3.4.7 MobileTwoFactorContract.....	39
83	3.4.8 Password.....	42
84	3.4.9 PasswordProtectedTransport.....	44
85	3.4.10 PreviousSession.....	45
86	3.4.11 Public Key – X.509.....	47
87	3.4.12 Public Key – PGP.....	48
88	3.4.13 Public Key – SPKI.....	50
89	3.4.14 Public Key - XML Digital Signature.....	52
90	3.4.15 Smartcard.....	53
91	3.4.16 SmartcardPKI.....	55
92	3.4.17 SoftwarePKI.....	57
93	3.4.18 Telephony.....	59
94	3.4.19 Telephony ("Nomadic").....	61
95	3.4.20 Telephony (Personalized).....	62
96	3.4.21 Telephony (Authenticated).....	64
97	3.4.22 Secure Remote Password.....	65
98	3.4.23 SSL/TLS Certificate-Based Client Authentication.....	67
99	3.4.24 TimeSyncToken.....	69
100	3.4.25 Unspecified.....	71
101	4 References.....	72
102		

---

# 1 Introduction

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

## 1.1 Authentication Context Concepts

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

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

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

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

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

## 1.2 Notation and Terminology

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

139 `Listings of XML schemas appear like this.`

140 `Example code listings appear like this.`

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

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

Prefix	XML Namespace	Comments
ac:	urn:oasis:names:tc:SAML:2.0:ac	This is the namespace defined in this specification and in a schema [SAMLAC-xsd].
xs:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown. For clarity, the prefix is generally shown in specification text when XML Schema-related constructs are mentioned.
xsi:	http://www.w3.org/2001/XMLSchema-instance	This namespace is defined in the W3C XML Schema specification [Schema1] for schema-related markup that appears in XML instances.

150

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

---

## 2 Authentication Context Declaration

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

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

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

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

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

### 2.1 Data Model

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

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

## 195 2.2 Extensibility

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

## 201 2.3 Processing Rules

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

## 204 2.4 Schema

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

```
208 <?xml version="1.0" encoding="UTF-8"?>
209 <xs:schema
210   xmlns:xs="http://www.w3.org/2001/XMLSchema"
211   elementFormDefault="qualified">
212
213   <xs:annotation>
214     <xs:documentation>
215       Document identifier: sstc-saml-schema-authn-context-types-2.0
216       Location: http://www.oasis-
217 open.org/committees/documents.php?wg_abbrev=security
218       Revision history:
219         V2.0 CD-03 (December, 2004):
220         New core authentication context schema types for SAML V2.0.
221     </xs:documentation>
222   </xs:annotation>
223
224   <xs:element name="AuthenticationContextDeclaration"
225     type="AuthnContextDeclarationBaseType">
226     <xs:annotation>
227       <xs:documentation>
228         A particular assertion on an identity
229         provider's part with respect to the authentication
230         context associated with an authentication assertion.
231       </xs:documentation>
232     </xs:annotation>
233   </xs:element>
234
235   <xs:element name="Identification" type="IdentificationType">
236     <xs:annotation>
237       <xs:documentation>
238         Refers to those characteristics that describe the
239         processes and mechanisms
240         the Authentication Authority uses to initially create
241         an association between a Principal
242         and the identity (or name) by which the Principal will
243         be known
244       </xs:documentation>
245     </xs:annotation>
246   </xs:element>
247
248   <xs:element name="PhysicalVerification">
249     <xs:annotation>
250       <xs:documentation>
251         This element indicates that identification has been
```

```

252         performed in a physical
253         face-to-face meeting with the principal and not in an
254         online manner.
255     </xs:documentation>
256 </xs:annotation>
257 <xs:complexType>
258     <xs:attribute name="credentialLevel">
259         <xs:simpleType>
260             <xs:restriction base="xs:NMTOKEN">
261                 <xs:enumeration value="primary"/>
262                 <xs:enumeration value="secondary"/>
263             </xs:restriction>
264         </xs:simpleType>
265     </xs:attribute>
266 </xs:complexType>
267 </xs:element>
268
269 <xs:element name="WrittenConsent">
270     <xs:complexType>
271         <xs:sequence>
272             <xs:element ref="Extension" minOccurs="0"
273                 maxOccurs="unbounded"/>
274         </xs:sequence>
275     </xs:complexType>
276 </xs:element>
277
278 <xs:element name="TechnicalProtection"
279     type="TechnicalProtectionBaseType">
280     <xs:annotation>
281         <xs:documentation>
282             Refers to those characteristics that describe how the
283             'secret' (the knowledge or possession
284             of which allows the Principal to authenticate to the
285             Authentication Authority) is kept secure
286         </xs:documentation>
287     </xs:annotation>
288 </xs:element>
289
290 <xs:element name="SecretKeyProtection"
291     type="SecretKeyProtectionType">
292     <xs:annotation>
293         <xs:documentation>
294             This element indicates the types and strengths of
295             facilities
296             of a UA used to protect a shared secret key from
297             unauthorized access and/or use.
298         </xs:documentation>
299     </xs:annotation>
300 </xs:element>
301
302 <xs:element name="PrivateKeyProtection"
303     type="PrivateKeyProtectionType">
304     <xs:annotation>
305         <xs:documentation>
306             This element indicates the types and strengths of
307             facilities
308             of a UA used to protect a private key from
309             unauthorized access and/or use.
310         </xs:documentation>
311     </xs:annotation>
312 </xs:element>
313
314 <xs:element name="KeyActivation" type="KeyActivationType">
315     <xs:annotation>
316         <xs:documentation>The actions that must be performed
317         before the private key can be used. </xs:documentation>
318     </xs:annotation>

```



```

319 </xs:element>
320
321 <xs:element name="KeySharing" type="KeySharingType">
322   <xs:annotation>
323     <xs:documentation>Whether or not the private key is shared
324       with the certificate authority.</xs:documentation>
325   </xs:annotation>
326 </xs:element>
327
328 <xs:element name="KeyStorage" type="KeyStorageType">
329   <xs:annotation>
330     <xs:documentation>
331       In which medium is the key stored.
332       memory - the key is stored in memory.
333       smartcard - the key is stored in a smartcard.
334       token - the key is stored in a hardware token.
335       MobileDevice - the key is stored in a mobile device.
336       MobileAuthCard - the key is stored in a mobile
337       authentication card.
338     </xs:documentation>
339   </xs:annotation>
340 </xs:element>
341
342 <xs:element name="SubscriberLineNumber">
343   <xs:complexType>
344     <xs:sequence>
345       <xs:element ref="Extension" minOccurs="0"
346         maxOccurs="unbounded"/>
347     </xs:sequence>
348   </xs:complexType>
349 </xs:element>
350
351 <xs:element name="UserSuffix">
352   <xs:complexType>
353     <xs:sequence>
354       <xs:element ref="Extension" minOccurs="0"
355         maxOccurs="unbounded"/>
356     </xs:sequence>
357   </xs:complexType>
358 </xs:element>
359
360 <xs:element name="Password" type="PasswordType">
361   <xs:annotation>
362     <xs:documentation>
363       This element indicates that a password (or passphrase)
364       has been used to
365       authenticate the Principal to a remote system.
366     </xs:documentation>
367   </xs:annotation>
368 </xs:element>
369
370 <xs:element name="ActivationPin" type="ActivationPinType">
371   <xs:annotation>
372     <xs:documentation>
373       This element indicates that a Pin (Personal
374       Identification Number) has been used to authenticate the
375       Principal to
376       some local system in order to activate a key.
377     </xs:documentation>
378   </xs:annotation>
379 </xs:element>
380
381 <xs:element name="Token" type="TokenType">
382   <xs:annotation>
383     <xs:documentation>
384       This element indicates that a hardware or software
385       token is used

```

```

386         as a method of identifying the Principal.
387     </xs:documentation>
388 </xs:annotation>
389 </xs:element>
390
391 <xs:element name="TimeSyncToken" type="TimeSyncTokenType">
392     <xs:annotation>
393         <xs:documentation>
394             This element indicates that a time synchronization
395             token is used to identify the Principal. hardware -
396             the time synchronization
397             token has been implemented in hardware. software - the
398             time synchronization
399             token has been implemented in software. SeedLength -
400             the length, in bits, of the
401             random seed used in the time synchronization token.
402         </xs:documentation>
403     </xs:annotation>
404 </xs:element>
405
406 <xs:element name="Smartcard">
407     <xs:annotation>
408         <xs:documentation>
409             This element indicates that a smartcard is used to
410             identity the Principal.
411         </xs:documentation>
412     </xs:annotation>
413     <xs:complexType>
414         <xs:sequence>
415             <xs:element ref="Extension" minOccurs="0"
416                 maxOccurs="unbounded"/>
417         </xs:sequence>
418     </xs:complexType>
419 </xs:element>
420
421 <xs:element name="Length" type="LengthType">
422     <xs:annotation>
423         <xs:documentation>
424             This element indicates the minimum and/or maximum
425             ASCII length of the password which is enforced (by the UA or the
426             IdP). In other words, this is the minimum and/or maximum number
427 of ASCII characters required to represent a valid password.
428             min - the minimum number of ASCII characters required
429             in a valid password, as enforced by the UA or the IdP.
430             max - the maximum number of ASCII characters required
431             in a valid password, as enforced by the UA or the IdP.
432         </xs:documentation>
433     </xs:annotation>
434 </xs:element>
435
436 <xs:element name="ActivationLimit" type="ActivationLimitType">
437     <xs:annotation>
438         <xs:documentation>
439             This element indicates the length of time for which an
440             PIN-based authentication is valid.
441         </xs:documentation>
442     </xs:annotation>
443 </xs:element>
444
445 <xs:element name="Generation">
446     <xs:annotation>
447         <xs:documentation>
448             Indicates whether the password was chosen by the
449             Principal or auto-supplied by the Authentication Authority.
450             principalchosen - the Principal is allowed to choose
451             the value of the password. This is true even if
452

```

```

453         the initial password is chosen at random by the UA or
454         the IdP and the Principal is then free to change
455         the password.
456         automatic - the password is chosen by the UA or the
457         IdP to be cryptographically strong in some sense,
458         or to satisfy certain password rules, and that the
459         Principal is not free to change it or to choose a new password.
460     </xs:documentation>
461 </xs:annotation>
462
463     <xs:complexType>
464         <xs:attribute name="mechanism" use="required">
465             <xs:simpleType>
466                 <xs:restriction base="xs:NMTOKEN">
467                     <xs:enumeration value="principalchosen"/>
468                     <xs:enumeration value="automatic"/>
469                 </xs:restriction>
470             </xs:simpleType>
471         </xs:attribute>
472     </xs:complexType>
473 </xs:element>
474
475 <xs:element name="AuthnMethod"
476     type="AuthnMethodBaseType">
477     <xs:annotation>
478         <xs:documentation>
479             Refers to those characteristics that define the
480             mechanisms by which the Principal authenticates to the
481 Authentication
482             Authority.
483         </xs:documentation>
484     </xs:annotation>
485 </xs:element>
486
487 <xs:element name="PrincipalAuthenticationMechanism"
488     type="PrincipalAuthenticationMechanismType">
489     <xs:annotation>
490         <xs:documentation>
491             The method that a Principal employs to perform
492             authentication to local system components.
493         </xs:documentation>
494     </xs:annotation>
495 </xs:element>
496
497 <xs:element name="Authenticator" type="AuthenticatorBaseType">
498     <xs:annotation>
499         <xs:documentation>
500             The method applied to validate a principal's
501             authentication across a network
502         </xs:documentation>
503     </xs:annotation>
504 </xs:element>
505
506 <xs:element name="PreviousSession">
507     <xs:annotation>
508         <xs:documentation>
509             Indicates that the Principal has been strongly
510             authenticated in a previous session during which the IdP has set
511 a
512             cookie in the UA. During the present session the Principal has
513 only
514             been authenticated by the UA returning the cookie to the IdP.
515         </xs:documentation>
516     </xs:annotation>
517 <xs:complexType>
518     <xs:sequence>
519         <xs:element ref="Extension" minOccurs="0"

```

```

520         maxOccurs="unbounded"/>
521     </xs:sequence>
522 </xs:complexType>
523 </xs:element>
524
525 <xs:element name="ResumeSession">
526     <xs:annotation>
527         <xs:documentation>
528             Rather like PreviousSession but using stronger
529             security. A secret that was established in a previous session
530 with
531         the Authentication Authority has been cached by the local system
532 and
533         is now re-used (e.g. a Master Secret is used to derive new
534 session
535         keys in TLS, SSL, WTLS).
536     </xs:documentation>
537 </xs:annotation>
538 <xs:complexType>
539     <xs:sequence>
540         <xs:element ref="Extension" minOccurs="0"
541             maxOccurs="unbounded"/>
542     </xs:sequence>
543 </xs:complexType>
544 </xs:element>
545
546 <xs:element name="ZeroKnowledge">
547     <xs:annotation>
548         <xs:documentation>
549             This element indicates that the Principal has been
550             authenticated by a zero knowledge technique as specified in
551 ISO/IEC
552             9798-5.
553         </xs:documentation>
554     </xs:annotation>
555 <xs:complexType>
556     <xs:sequence>
557         <xs:element ref="Extension" minOccurs="0"
558             maxOccurs="unbounded"/>
559     </xs:sequence>
560 </xs:complexType>
561 </xs:element>
562
563 <xs:element name="SharedSecretChallengeResponse"
564 type="SharedSecretChallengeResponseType"/>
565
566 <xs:complexType name="SharedSecretChallengeResponseType">
567     <xs:annotation>
568         <xs:documentation>
569             This element indicates that the Principal has been
570             authenticated by a challenge-response protocol utilizing shared
571 secret
572             keys and symmetric cryptography.
573         </xs:documentation>
574     </xs:annotation>
575 <xs:sequence>
576         <xs:element ref="Extension" minOccurs="0"
577             maxOccurs="unbounded"/>
578     </xs:sequence>
579     <xs:attribute name="method" type="xs:anyURI" use="optional"/>
580 </xs:complexType>
581
582 <xs:element name="DigSig" type="PublicKeyType">
583     <xs:annotation>
584         <xs:documentation>
585             This element indicates that the Principal has been

```

```

586         authenticated by a mechanism which involves the Principal
587 computing a
588         digital signature over at least challenge data provided by the
589 IdP.
590     </xs:documentation>
591 </xs:annotation>
592 </xs:element>
593
594 <xs:element name="AsymmetricDecryption" type="PublicKeyType">
595     <xs:annotation>
596         <xs:documentation>
597             The local system has a private key but it is used
598             in decryption mode, rather than signature mode. For example, the
599             Authentication Authority generates a secret and encrypts it using
600 the
601             local system's public key: the local system then proves it has
602             decrypted the secret.
603         </xs:documentation>
604     </xs:annotation>
605 </xs:element>
606
607 <xs:element name="AsymmetricKeyAgreement" type="PublicKeyType">
608     <xs:annotation>
609         <xs:documentation>
610             The local system has a private key and uses it for
611             shared secret key agreement with the Authentication Authority
612 (e.g.
613             via Diffie Helman).
614         </xs:documentation>
615     </xs:annotation>
616 </xs:element>
617
618 <xs:complexType name="PublicKeyType">
619     <xs:sequence>
620         <xs:element ref="Extension" minOccurs="0"
621             maxOccurs="unbounded"/>
622     </xs:sequence>
623     <xs:attribute name="keyValidation" use="optional"/>
624 </xs:complexType>
625
626 <xs:element name="IPAddress">
627     <xs:annotation>
628         <xs:documentation>
629             This element indicates that the Principal has been
630             authenticated through connection from a particular IP address.
631         </xs:documentation>
632     </xs:annotation>
633 <xs:complexType>
634     <xs:sequence>
635         <xs:element ref="Extension" minOccurs="0"
636             maxOccurs="unbounded"/>
637     </xs:sequence>
638 </xs:complexType>
639 </xs:element>
640
641 <xs:element name="SharedSecretDynamicPlaintext"
642 type="SharedSecretDynamicPlaintextType"/>
643
644 <xs:annotation>
645     <xs:documentation>
646         The local system and Authentication Authority
647         share a secret key. The local system uses this to encrypt a
648         randomised string to pass to the Authentication Authority.
649     </xs:documentation>
650 </xs:annotation>
651
652 <xs:complexType name="SharedSecretDynamicPlaintextType">

```

```

653     <xs:sequence>
654         <xs:element ref="Extension" minOccurs="0"
655             maxOccurs="unbounded"/>
656     </xs:sequence>
657 </xs:complexType>
658
659 <xs:element name="AuthenticatorTransportProtocol"
660     type="AuthenticatorTransportProtocolType">
661     <xs:annotation>
662         <xs:documentation>
663             The protocol across which Authenticator information is
664             transferred to an Authentication Authority verifier.
665         </xs:documentation>
666     </xs:annotation>
667 </xs:element>
668
669 <xs:element name="HTTP">
670     <xs:annotation>
671         <xs:documentation>
672             This element indicates that the Authenticator has been
673             transmitted using bare HTTP utilizing no additional security
674             protocols.
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
685 <xs:element name="IPSec">
686     <xs:annotation>
687         <xs:documentation>
688             This element indicates that the Authenticator has been
689             transmitted using a transport mechanism protected by an IPSEC
690             session.
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="WTLS">
701     <xs:annotation>
702         <xs:documentation>
703             This element indicates that the Authenticator has been
704             transmitted using a transport mechanism protected by a WTLS
705             session.
706         </xs:documentation>
707     </xs:annotation>
708 <xs:complexType>
709     <xs:sequence>
710         <xs:element ref="Extension" minOccurs="0"
711             maxOccurs="unbounded"/>
712     </xs:sequence>
713 </xs:complexType>
714 </xs:element>
715 <xs:element name="MobileNetworkNoEncryption">
716     <xs:annotation>
717         <xs:documentation>
718             This element indicates that the Authenticator has been
719             transmitted solely across a mobile network using no additional

```

```

720         security mechanism.
721     </xs:documentation>
722 </xs:annotation>
723 <xs:complexType>
724     <xs:sequence>
725         <xs:element ref="Extension" minOccurs="0"
726             maxOccurs="unbounded"/>
727     </xs:sequence>
728 </xs:complexType>
729 </xs:element>
730 <xs:element name="MobileNetworkRadioEncryption">
731     <xs:complexType>
732         <xs:sequence>
733             <xs:element ref="Extension" minOccurs="0"
734                 maxOccurs="unbounded"/>
735         </xs:sequence>
736     </xs:complexType>
737 </xs:element>
738 <xs:element name="MobileNetworkEndToEndEncryption">
739     <xs:complexType>
740         <xs:sequence>
741             <xs:element ref="Extension" minOccurs="0"
742                 maxOccurs="unbounded"/>
743         </xs:sequence>
744     </xs:complexType>
745 </xs:element>
746
747 <xs:element name="SSL">
748     <xs:annotation>
749         <xs:documentation>
750             This element indicates that the Authenticator has been
751             transmitted using a transport mechanism protected by an SSL or
752             TLS
753             session.
754         </xs:documentation>
755     </xs:annotation>
756     <xs:complexType>
757         <xs:sequence>
758             <xs:element ref="Extension" minOccurs="0"
759                 maxOccurs="unbounded"/>
760         </xs:sequence>
761     </xs:complexType>
762 </xs:element>
763
764 <xs:element name="PSTN">
765     <xs:complexType>
766         <xs:sequence>
767             <xs:element ref="Extension" minOccurs="0"
768                 maxOccurs="unbounded"/>
769         </xs:sequence>
770     </xs:complexType>
771 </xs:element>
772
773 <xs:element name="ISDN">
774     <xs:complexType>
775         <xs:sequence>
776             <xs:element ref="Extension" minOccurs="0"
777                 maxOccurs="unbounded"/>
778         </xs:sequence>
779     </xs:complexType>
780 </xs:element>
781
782 <xs:element name="ADSL">
783     <xs:complexType>
784         <xs:sequence>
785             <xs:element ref="Extension" minOccurs="0"
786                 maxOccurs="unbounded"/>

```

```

787     </xs:sequence>
788   </xs:complexType>
789 </xs:element>
790
791   <xs:element name="OperationalProtection"
792     type="OperationalProtectionType">
793     <xs:annotation>
794       <xs:documentation>
795         Refers to those characteristics that describe
796         procedural security controls employed by the Authentication
797 Authority.
798       </xs:documentation>
799     </xs:annotation>
800   </xs:element>
801
802   <xs:element name="SecurityAudit" type="SecurityAuditType"/>
803
804   <xs:element name="SwitchAudit">
805     <xs:complexType>
806       <xs:sequence>
807         <xs:element ref="Extension" minOccurs="0"
808           maxOccurs="unbounded"/>
809       </xs:sequence>
810     </xs:complexType>
811   </xs:element>
812
813   <xs:element name="DeactivationCallCenter">
814     <xs:complexType>
815       <xs:sequence>
816         <xs:element ref="Extension" minOccurs="0"
817           maxOccurs="unbounded"/>
818       </xs:sequence>
819     </xs:complexType>
820   </xs:element>
821
822   <xs:element name="GoverningAgreements"
823     type="GoverningAgreementsType">
824     <xs:annotation>
825       <xs:documentation>
826         Provides a mechanism for linking to external (likely
827         human readable) documents in which additional business
828 agreements,
829         (e.g. liability constraints, obligations, etc) can be placed.
830       </xs:documentation>
831     </xs:annotation>
832   </xs:element>
833
834   <xs:element name="GoverningAgreementRef"
835     type="GoverningAgreementRefType"/>
836
837   <xs:simpleType name="nymType">
838     <xs:restriction base="xs:NMTOKEN">
839       <xs:enumeration value="anonymity"/>
840       <xs:enumeration value="verinymity"/>
841       <xs:enumeration value="pseudonymity"/>
842     </xs:restriction>
843   </xs:simpleType>
844
845   <xs:complexType name="IdentificationType">
846     <xs:sequence>
847       <xs:element ref="PhysicalVerification" minOccurs="0"/>
848       <xs:element ref="WrittenConsent" minOccurs="0"/>
849       <xs:element ref="GoverningAgreements" minOccurs="0"/>
850       <xs:element ref="Extension" minOccurs="0"
851         maxOccurs="unbounded"/>
852     </xs:sequence>
853   <xs:attribute name="nym" type="nymType">

```



```

854     <xs:annotation>
855       <xs:documentation>
856         This attribute indicates whether or not the
857         Identification mechanisms allow the actions of the Principal to
858 be
859         linked to an actual end user.
860       </xs:documentation>
861     </xs:annotation>
862   </xs:attribute>
863 </xs:complexType>
864
865 <xs:complexType name="GoverningAgreementsType">
866   <xs:sequence>
867     <xs:element ref="GoverningAgreementRef"
868       maxOccurs="unbounded"/>
869   </xs:sequence>
870 </xs:complexType>
871
872 <xs:complexType name="GoverningAgreementRefType">
873   <xs:attribute name="governingAgreementRef" type="xs:anyURI"
874     use="required"/>
875 </xs:complexType>
876
877 <xs:complexType name="AuthenticatorTransportProtocolType">
878   <xs:choice>
879     <xs:element ref="HTTP"/>
880     <xs:element ref="SSL"/>
881     <xs:element ref="MobileNetworkNoEncryption"/>
882     <xs:element ref="MobileNetworkRadioEncryption"/>
883     <xs:element ref="MobileNetworkEndToEndEncryption"/>
884     <xs:element ref="WTLS"/>
885     <xs:element ref="IPSec"/>
886     <xs:element ref="PSTN"/>
887     <xs:element ref="ISDN"/>
888     <xs:element ref="ADSL"/>
889     <xs:element ref="Extension" minOccurs="0"
890       maxOccurs="unbounded"/>
891   </xs:choice>
892 </xs:complexType>
893
894 <xs:complexType name="PrincipalAuthenticationMechanismType">
895   <xs:sequence>
896     <xs:choice>
897       <xs:element ref="Password"/>
898       <xs:element ref="Token"/>
899       <xs:element ref="Smartcard"/>
900       <xs:element ref="ActivationPin"/>
901       <xs:element ref="Extension" minOccurs="0"
902         maxOccurs="unbounded"/>
903     </xs:choice>
904   </xs:sequence>
905   <xs:attribute name="preauth" type="xs:integer" use="optional"/>
906 </xs:complexType>
907
908 <xs:complexType name="AuthnMethodBaseType">
909   <xs:sequence>
910     <xs:element ref="PrincipalAuthenticationMechanism"
911       minOccurs="0"/>
912     <xs:element ref="Authenticator" minOccurs="0"/>
913     <xs:element ref="AuthenticatorTransportProtocol"
914       minOccurs="0"/>
915     <xs:element ref="Extension" minOccurs="0"
916       maxOccurs="unbounded"/>
917   </xs:sequence>
918 </xs:complexType>
919
920 <xs:complexType name="AuthnContextDeclarationBaseType">

```

```

921 <xs:sequence>
922 <xs:element ref="Identification" minOccurs="0"/>
923 <xs:element ref="TechnicalProtection" minOccurs="0"/>
924 <xs:element ref="OperationalProtection" minOccurs="0"/>
925 <xs:element ref="AuthnMethod" minOccurs="0"/>
926 <xs:element ref="GoverningAgreements" minOccurs="0"/>
927 <xs:element ref="Extension" minOccurs="0"
928     maxOccurs="unbounded"/>
929 </xs:sequence>
930 <xs:attribute name="ID" type="xs:ID"/>
931 </xs:complexType>
932
933 <xs:complexType name="TechnicalProtectionBaseType">
934 <xs:choice>
935 <xs:element ref="PrivateKeyProtection"/>
936 <xs:element ref="SecretKeyProtection"/>
937 <xs:element ref="Extension" minOccurs="0"
938     maxOccurs="unbounded"/>
939 </xs:choice>
940 </xs:complexType>
941
942 <xs:complexType name="OperationalProtectionType">
943 <xs:sequence>
944 <xs:element ref="SecurityAudit" minOccurs="0"/>
945 <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
946 <xs:element ref="Extension" minOccurs="0"
947     maxOccurs="unbounded"/>
948 </xs:sequence>
949 </xs:complexType>
950
951 <xs:complexType name="AuthenticatorBaseType">
952 <xs:choice>
953 <xs:element ref="AuthenticatorChoice" minOccurs="1"/>
954 <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
955 </xs:choice>
956 </xs:complexType>
957
958 <xs:element name="AuthenticatorChoice" type="AuthenticatorChoiceType"/>
959 <xs:element name="AuthenticatorSequence"
960 type="AuthenticatorSequenceType"/>
961
962 <xs:complexType name="AuthenticatorSequenceType">
963 <xs:sequence>
964 <xs:element ref="PreviousSession" minOccurs="0"/>
965 <xs:element ref="ResumeSession" minOccurs="0"/>
966 <xs:element ref="DigSig" minOccurs="0"/>
967 <xs:element ref="Password" minOccurs="0"/>
968 <xs:element ref="RestrictedPassword" minOccurs="0"/>
969 <xs:element ref="ZeroKnowledge" minOccurs="0"/>
970 <xs:element ref="SharedSecretChallengeResponse" minOccurs="0"/>
971 <xs:element ref="SharedSecretDynamicPlaintext" minOccurs="0"/>
972 <xs:element ref="IPAddress" minOccurs="0"/>
973 <xs:element ref="AsymmetricDecryption" minOccurs="0"/>
974 <xs:element ref="AsymmetricKeyAgreement" minOccurs="0"/>
975 <xs:element ref="SubscriberLineNumber" minOccurs="0"/>
976 <xs:element ref="UserSuffix" minOccurs="0"/>
977 <xs:element ref="Extension" minOccurs="0"
978     maxOccurs="unbounded"/>
979 </xs:sequence>
980 </xs:complexType>
981
982 <xs:complexType name="AuthenticatorChoiceType">
983 <xs:choice>
984 <xs:element ref="PreviousSession" minOccurs="0"/>
985 <xs:element ref="ResumeSession" minOccurs="0"/>
986 <xs:element ref="DigSig" minOccurs="0"/>
987 <xs:element ref="Password" minOccurs="0"/>

```

```

988     <xs:element ref="RestrictedPassword" minOccurs="0"/>
989     <xs:element ref="ZeroKnowledge" minOccurs="0"/>
990     <xs:element ref="SharedSecretChallengeResponse" minOccurs="0"/>
991     <xs:element ref="SharedSecretDynamicPlaintext" minOccurs="0"/>
992     <xs:element ref="IPAddress" minOccurs="0"/>
993     <xs:element ref="AsymmetricDecryption" minOccurs="0"/>
994     <xs:element ref="AsymmetricKeyAgreement" minOccurs="0"/>
995     <xs:element ref="SubscriberLineNumber" minOccurs="0"/>
996     <xs:element ref="UserSuffix" minOccurs="0"/>
997     <xs:element ref="Extension" minOccurs="0"
998         maxOccurs="unbounded"/>
999     </xs:choice>
1000 </xs:complexType>
1001
1002 <xs:complexType name="KeyActivationType">
1003     <xs:choice>
1004         <xs:element ref="ActivationPin"/>
1005         <xs:element ref="Extension" minOccurs="0"
1006             maxOccurs="unbounded"/>
1007     </xs:choice>
1008 </xs:complexType>
1009
1010 <xs:complexType name="KeySharingType">
1011     <xs:attribute name="sharing" type="xs:boolean"
1012         use="required"/>
1013 </xs:complexType>
1014
1015 <xs:complexType name="PrivateKeyProtectionType">
1016     <xs:sequence>
1017         <xs:element ref="KeyActivation" minOccurs="0"/>
1018         <xs:element ref="KeyStorage" minOccurs="0"/>
1019         <xs:element ref="KeySharing" minOccurs="0"/>
1020         <xs:element ref="Extension" minOccurs="0"
1021             maxOccurs="unbounded"/>
1022     </xs:sequence>
1023 </xs:complexType>
1024
1025 <xs:complexType name="PasswordType">
1026     <xs:sequence>
1027         <xs:element ref="Length" minOccurs="0"/>
1028         <xs:element ref="Alphabet" minOccurs="0"/>
1029         <xs:element ref="Generation" minOccurs="0"/>
1030         <xs:element ref="Extension" minOccurs="0"
1031             maxOccurs="unbounded"/>
1032     </xs:sequence>
1033     <xs:attribute name="ExternalVerification" type="xs:anyURI"
1034         use="optional"/>
1035 </xs:complexType>
1036
1037 <xs:element name="RestrictedPassword" type="RestrictedPasswordType"/>
1038
1039 <xs:complexType name="RestrictedPasswordType">
1040     <xs:complexContent>
1041         <xs:restriction base="PasswordType">
1042             <xs:sequence>
1043                 <xs:element name="Length" type="RestrictedLengthType"
1044                     minOccurs="1"/>
1045                 <xs:element ref="Generation" minOccurs="0"/>
1046                 <xs:element ref="Extension" minOccurs="0"
1047                     maxOccurs="unbounded"/>
1048             </xs:sequence>
1049             <xs:attribute name="ExternalVerification" type="xs:anyURI"
1050                 use="optional"/>
1051         </xs:restriction>
1052     </xs:complexContent>
1053 </xs:complexType>
1054

```

```

1055 <xs:complexType name="RestrictedLengthType">
1056   <xs:complexContent>
1057     <xs:restriction base="LengthType">
1058       <xs:attribute name="min" use="required">
1059         <xs:simpleType>
1060           <xs:restriction base="xs:integer">
1061             <xs:minInclusive value="3"/>
1062           </xs:restriction>
1063         </xs:simpleType>
1064       </xs:attribute>
1065       <xs:attribute name="max" type="xs:integer" use="optional"/>
1066     </xs:restriction>
1067   </xs:complexContent>
1068 </xs:complexType>
1069
1070 <xs:complexType name="ActivationPinType">
1071   <xs:sequence>
1072     <xs:element ref="Length" minOccurs="0"/>
1073     <xs:element ref="Alphabet" minOccurs="0"/>
1074     <xs:element ref="Generation" minOccurs="0"/>
1075     <xs:element ref="ActivationLimit" minOccurs="0"/>
1076     <xs:element ref="Extension" minOccurs="0"
1077       maxOccurs="unbounded"/>
1078   </xs:sequence>
1079 </xs:complexType>
1080 <xs:element name="Alphabet" type="AlphabetType"/>
1081 <xs:complexType name="AlphabetType">
1082   <xs:attribute name="requiredChars" type="xs:string"
1083     use="required"/>
1084   <xs:attribute name="excludedChars" type="xs:string"
1085     use="optional"/>
1086   <xs:attribute name="case" type="xs:string" use="optional"/>
1087 </xs:complexType>
1088 <xs:complexType name="TokenType">
1089   <xs:sequence>
1090     <xs:element ref="TimeSyncToken"/>
1091     <xs:element ref="Extension" minOccurs="0"
1092       maxOccurs="unbounded"/>
1093   </xs:sequence>
1094 </xs:complexType>
1095 <xs:simpleType name="DeviceTypeType">
1096   <xs:restriction base="xs:NMTOKEN">
1097     <xs:enumeration value="hardware"/>
1098     <xs:enumeration value="software"/>
1099   </xs:restriction>
1100 </xs:simpleType>
1101 <xs:simpleType name="booleanType">
1102   <xs:restriction base="xs:NMTOKEN">
1103     <xs:enumeration value="true"/>
1104     <xs:enumeration value="false"/>
1105   </xs:restriction>
1106 </xs:simpleType>
1107 <xs:complexType name="TimeSyncTokenType">
1108   <xs:attribute name="DeviceType" type="DeviceTypeType"
1109     use="required"/>
1110   <xs:attribute name="SeedLength" type="xs:integer"
1111     use="required"/>
1112   <xs:attribute name="DeviceInHand" type="booleanType" use="required"/>
1113 </xs:complexType>
1114 <xs:complexType name="ActivationLimitType">
1115   <xs:choice>
1116     <xs:element ref="ActivationLimitDuration"/>
1117     <xs:element ref="ActivationLimitUsages"/>
1118     <xs:element ref="ActivationLimitSession"/>
1119   </xs:choice>
1120 </xs:complexType>
1121 <xs:element name="ActivationLimitDuration"

```

```

1122     type="ActivationLimitDurationType">
1123     <xs:annotation>
1124         <xs:documentation>
1125             This element indicates that the Key Activation Limit is
1126             defined as a specific duration of time.
1127         </xs:documentation>
1128     </xs:annotation>
1129 </xs:element>
1130 <xs:element name="ActivationLimitUsages"
1131     type="ActivationLimitUsagesType">
1132     <xs:annotation>
1133         <xs:documentation>
1134             This element indicates that the Key Activation Limit is
1135             defined as a number of usages.
1136         </xs:documentation>
1137     </xs:annotation>
1138 </xs:element>
1139 <xs:element name="ActivationLimitSession"
1140     type="ActivationLimitSessionType">
1141     <xs:annotation>
1142         <xs:documentation>
1143             This element indicates that the Key Activation Limit is
1144             the session.
1145         </xs:documentation>
1146     </xs:annotation>
1147 </xs:element>
1148 <xs:complexType name="ActivationLimitDurationType">
1149     <xs:attribute name="duration" type="xs:duration"
1150         use="required"/>
1151 </xs:complexType>
1152 <xs:complexType name="ActivationLimitUsagesType">
1153     <xs:attribute name="number" type="xs:integer"
1154         use="required"/>
1155 </xs:complexType>
1156 <xs:complexType name="ActivationLimitSessionType"/>
1157 <xs:complexType name="LengthType">
1158     <xs:attribute name="min" type="xs:integer" use="required"/>
1159     <xs:attribute name="max" type="xs:integer" use="optional"/>
1160 </xs:complexType>
1161
1162 <xs:simpleType name="mediumType">
1163     <xs:restriction base="xs:NMTOKEN">
1164         <xs:enumeration value="memory"/>
1165         <xs:enumeration value="smartcard"/>
1166         <xs:enumeration value="token"/>
1167         <xs:enumeration value="MobileDevice"/>
1168         <xs:enumeration value="MobileAuthCard"/>
1169     </xs:restriction>
1170 </xs:simpleType>
1171
1172 <xs:complexType name="KeyStorageType">
1173     <xs:attribute name="medium" type="mediumType" use="required"/>
1174 </xs:complexType>
1175
1176 <xs:complexType name="SecretKeyProtectionType">
1177     <xs:sequence>
1178         <xs:element ref="KeyActivation" minOccurs="0"/>
1179         <xs:element ref="KeyStorage" minOccurs="0"/>
1180         <xs:element ref="Extension" minOccurs="0"
1181             maxOccurs="unbounded"/>
1182     </xs:sequence>
1183 </xs:complexType>
1184
1185 <xs:complexType name="SecurityAuditType">
1186     <xs:sequence>
1187         <xs:element ref="SwitchAudit" minOccurs="0"/>
1188         <xs:element ref="Extension" minOccurs="0"

```

```
1189         maxOccurs="unbounded"/>
1190     </xs:sequence>
1191 </xs:complexType>
1192
1193     <xs:element name="Extension" type="ExtensionType"/>
1194
1195     <xs:complexType name="ExtensionType">
1196         <xs:sequence>
1197             <xs:any namespace="##other" processContents="lax"
1198 maxOccurs="unbounded"/>
1199         </xs:sequence>
1200     </xs:complexType>
1201
1202 </xs:schema>
1203
```

1204

1205

```
1206 <xs:schema
1207     targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
1208     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1209     xmlns="urn:oasis:names:tc:SAML:2.0:ac">
1210
1211     <xs:annotation>
1212         <xs:documentation>
1213             Document identifier: sstc-saml-schema-authn-context-2.0
1214             Location: http://www.oasis-
1215 open.org/committees/documents.php?wg_abbrev=security
1216             Revision history:
1217                 V2.0 CD-03 (December, 2004):
1218                 New core authentication context schema for SAML V2.0.
1219                 This is just an include of all types from the schema
1220                 referred to in the include statement below.
1221         </xs:documentation>
1222     </xs:annotation>
1223
1224     <xs:include schemaLocation="sstc-saml-schema-authn-context-types-
1225 2.0.xsd"/>
1226
1227 </xs:schema>
```

---

## 1228 **3 Authentication Context Classes**

1229 The number of permutations of different characteristics ensures that there is a theoretically infinite number  
1230 of unique authentication contexts. The implication is that, in theory, any particular relying party would be  
1231 expected to be able to parse arbitrary authentication context declarations and, more importantly, to  
1232 analyze the declaration in order to assess the “quality” of the associated authentication assertion. Making  
1233 such an assessment is non-trivial.

1234 Fortunately, an optimization is possible. In practice many authentication contexts will fall into categories  
1235 determined by industry practices and technology. For instance, many B2C web browser authentication  
1236 contexts will be (partially) defined by the principal authenticating to the authentication authority through the  
1237 presentation of a password over an SSL protected session. In the enterprise world, certificate-based  
1238 authentication will be more common. Of course, the full authentication context is not limited to the  
1239 specifics of how the principal authenticated. Nevertheless, the authentication method is often the most  
1240 visible characteristic and as such, can serve as a useful classifier for a class of related authentication  
1241 contexts.

1242 The concept is expressed in this specification as a definition of a series of authentication context classes.  
1243 Each class defines a proper subset of the full set of authentication contexts. Classes have been chosen  
1244 as representative of the current practices and technologies for authentication technologies, and provide  
1245 identity and service providers a convenient shorthand when referring to authentication context issues.

1246 For instance, an authentication authority may include with the complete authentication context declaration  
1247 it provides to a service provider an assertion that the authentication context also belongs to one of the  
1248 authentication classes defined here. For some service providers, this assertion is sufficient detail for it to  
1249 be able to assign an appropriate level of confidence to the associated authentication assertion. Other  
1250 service providers might prefer to examine the complete authentication context declaration itself. Likewise,  
1251 the ability to refer to an authentication context class rather than being required to list the complete details  
1252 of a specific authentication content will simplify how the service provider expresses its desires and/or  
1253 requirements to an authentication authority.

### 1254 **3.1 Advantages of Authentication Context Classes**

1255 The introduction of the additional layer of classes and the definition of an initial list of representative and  
1256 flexible classes are expected to:

- 1257 • Make it easier for the authentication authority and service provider to come to an agreement on what  
1258 are acceptable authentication contexts by giving them a framework for discussion.
- 1259 • Make it easier for service providers to indicate their preferences when requesting a step-up  
1260 authentication assertion from an authentication authority.
- 1261 • Simplify for service providers the burden of processing authentication context declarations by giving  
1262 them the option of being satisfied by the associated class.
- 1263 • Protect service providers from impact of new authentication technologies.
- 1264 • Make it easier for authentication authorities to publish their authentication capabilities, for example,  
1265 through WSDL.

### 1266 **3.2 Processing Rules**

1267 Further processing rules for authentication context classes are described in the SAML assertions and  
1268 protocols specification [SAMLCore].

## 1269 3.3 Extensibility

1270 As does the core authentication context declaration schema, the separate authentication context classes  
1271 schemas allow the `<Extension>` element in certain locations of the tree structure. In general, where the  
1272 `<Extension>` element occurred as a child of a `<Choice>` element, this option was removed in creating  
1273 the appropriate class schema definition as an extension of the base type. When the `<Extension>`  
1274 element occurred as an optional child of a `<Sequence>` element, the `<Extension>` element was  
1275 allowed to remain in addition to any required elements.

1276 Consequently, authentication context declarations can include the `<Extension>` element (with additional  
1277 elements in different namespaces) and still conform to authentication context class schemas (if they meet  
1278 the other requirements of the schema of course)

1279 The authentication context class schemas extend (as restrictions) appropriate type definitions in the core  
1280 authentication context declaration schema. As an extension point, the authentication context classes  
1281 schemas themselves can be extended – their type definitions serving as base types in some other  
1282 schema (potentially defined by some community wishing a more tightly defined authentication context  
1283 class). To prevent logical inconsistencies, any such extensions can only further constrain the type  
1284 definitions of the core authentication context declaration schema. To enforce this constraint, the  
1285 authentication context class schemas are defined with the `finalDefault="extension"` attribute on  
1286 the `<schema>` element to prevent this type of extension derivation.

1287 Additional authentication context classes MAY be developed by groups other than the Security Services  
1288 Technical Committee. OASIS members may wish to document and submit them for consideration by the  
1289 SSTC in a future version of the specification, and other groups may simply wish to inform the committee  
1290 of their work. Please refer to the SSTC web site for further details.

1291 Guidelines for the specification of new context classes are as follows:

- 1292 • Specify a URI that uniquely identifies the context class.
- 1293 • Provide contact information for the author of the class.
- 1294 • Provide a textual description of the circumstances under which this class should be used.
- 1295 • Provide a valid XML schema [Schema1] document implementing the class

1296 Authors of new classes are encouraged to review those classes defined within this specification in order to  
1297 guide their work.

## 1298 3.4 Schemas

1299 Authentication context classes are listed in the following subsections. The classes are listed in  
1300 alphabetical order; no other ranking is implied by the order of classes. Classes are uniquely identified by  
1301 URIs with the following initial stem:

```
1302 urn:oasis:names:tc:SAML:2.0:ac:classes
```

1303 The class schemas are defined as extension by restriction of parts of the the base authentication context  
1304 schema. XML instances that validate against a given authentication context class schema are said to  
1305 *conform* to that authentication context class.

### 1306 3.4.1 Internet Protocol

1307 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol

1308 Note that this URI is also used as the target namespace in the corresponding authentication context class  
1309 schema document [SAMLAC-IP]).

1310 The Internet Protocol class is identified when a Principal is authenticated through the use of a provided IP  
1311 address.



```

1312 <xs:schema
1313 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1314 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1315 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
1316 finalDefault="extension">
1317
1318   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
1319 2.0.xsd">
1320
1321     <xs:annotation>
1322       <xs:documentation>
1323         Class identifier:
1324 urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
1325         Document identifier: sstc-saml-schema-authn-context-ip-2.0
1326         Location: http://www.oasis-
1327 open.org/committees/documents.php?wg_abbrev=security
1328         Revision history:
1329           V2.0 CD-03 (December, 2004):
1330           New authentication context class schema for SAML V2.0.
1331       </xs:documentation>
1332     </xs:annotation>
1333
1334     <xs:complexType name="AuthnContextDeclarationBaseType">
1335       <xs:complexContent>
1336         <xs:restriction base="AuthnContextDeclarationBaseType">
1337           <xs:sequence>
1338             <xs:element ref="Identification" minOccurs="0"/>
1339             <xs:element ref="TechnicalProtection" minOccurs="0"/>
1340             <xs:element ref="OperationalProtection" minOccurs="0"/>
1341             <xs:element ref="AuthnMethod"/>
1342             <xs:element ref="GoverningAgreements" minOccurs="0"/>
1343             <xs:element ref="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:complexType name="AuthnMethodBaseType">
1352       <xs:complexContent>
1353         <xs:restriction base="AuthnMethodBaseType">
1354           <xs:sequence>
1355             <xs:element ref="PrincipalAuthenticationMechanism"
1356               minOccurs="0"/>
1357             <xs:element ref="Authenticator"/>
1358             <xs:element ref="AuthenticatorTransportProtocol"
1359               minOccurs="0"/>
1360             <xs:element ref="Extension" minOccurs="0"
1361               maxOccurs="unbounded"/>
1362           </xs:sequence>
1363         </xs:restriction>
1364       </xs:complexContent>
1365     </xs:complexType>
1366
1367     <xs:complexType name="AuthenticatorBaseType">
1368       <xs:complexContent>
1369         <xs:restriction base="AuthenticatorBaseType">
1370           <xs:choice>
1371             <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
1372           </xs:choice>
1373         </xs:restriction>
1374       </xs:complexContent>
1375     </xs:complexType>
1376
1377     <xs:complexType name="AuthenticatorSequenceType">
1378       <xs:complexContent>

```

```

1379     <xs:restriction base="AuthenticatorSequenceType">
1380         <xs:sequence>
1381             <xs:element ref="IPAddress"/>
1382         </xs:sequence>
1383     </xs:restriction>
1384 </xs:complexContent>
1385 </xs:complexType>
1386
1387 </xs:redefine>
1388
1389 </xs:schema>

```

### 1390 3.4.2 InternetProtocolPassword

1391 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword

1392 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 1393 schema document [SAMLAC-IPP]).

1394 The Internet Protocol Password class is identified when a Principal is authenticated through the use of a  
 1395 provided IP address, in addition to username/password.

```

1396 <xs:schema
1397 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolP
1398 assword"
1399   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
1400   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1401   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
1402   finalDefault="extension">
1403
1404   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
1405 2.0.xsd">
1406
1407     <xs:annotation>
1408       <xs:documentation>
1409         Class identifier:
1410 urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
1411         Document identifier: sstc-saml-schema-authn-context-ippword-2.0
1412         Location: http://www.oasis-
1413 open.org/committees/documents.php?wg_abbrev=security
1414         Revision history:
1415         V2.0 CD-03 (December, 2004):
1416         New authentication context class schema for SAML V2.0.
1417       </xs:documentation>
1418     </xs:annotation>
1419
1420     <xs:complexType name="AuthnContextDeclarationBaseType">
1421       <xs:complexContent>
1422         <xs:restriction base="AuthnContextDeclarationBaseType">
1423           <xs:sequence>
1424             <xs:element ref="Identification" minOccurs="0"/>
1425             <xs:element ref="TechnicalProtection" minOccurs="0"/>
1426             <xs:element ref="OperationalProtection" minOccurs="0"/>
1427             <xs:element ref="AuthnMethod"/>
1428             <xs:element ref="GoverningAgreements" minOccurs="0"/>
1429             <xs:element ref="Extension" minOccurs="0"
1430               maxOccurs="unbounded"/>
1431           </xs:sequence>
1432           <xs:attribute name="ID" type="xs:ID"/>
1433         </xs:restriction>
1434       </xs:complexContent>
1435     </xs:complexType>
1436
1437     <xs:complexType name="AuthnMethodBaseType">
1438       <xs:complexContent>
1439         <xs:restriction base="AuthnMethodBaseType">

```

```

1440         <xs:sequence>
1441             <xs:element ref="PrincipalAuthenticationMechanism"
1442 minOccurs="0"/>
1443             <xs:element ref="Authenticator"/>
1444             <xs:element ref="AuthenticatorTransportProtocol"
1445 minOccurs="0"/>
1446             <xs:element ref="Extension" minOccurs="0"
1447 maxOccurs="unbounded"/>
1448         </xs:sequence>
1449     </xs:restriction>
1450 </xs:complexContent>
1451 </xs:complexType>
1452
1453     <xs:complexType name="AuthenticatorBaseType">
1454         <xs:complexContent>
1455             <xs:restriction base="AuthenticatorBaseType">
1456                 <xs:choice>
1457                     <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
1458                 </xs:choice>
1459             </xs:restriction>
1460         </xs:complexContent>
1461     </xs:complexType>
1462
1463     <xs:complexType name="AuthenticatorSequenceType">
1464         <xs:complexContent>
1465             <xs:restriction base="AuthenticatorSequenceType">
1466                 <xs:sequence>
1467                     <xs:element ref="Password"/>
1468                     <xs:element ref="IPAddress"/>
1469                     <xs:element ref="Extension" minOccurs="0"
1470 maxOccurs="unbounded"/>
1471                 </xs:sequence>
1472             </xs:restriction>
1473         </xs:complexContent>
1474     </xs:complexType>
1475
1476 </xs:redefine>
1477
1478 </xs:schema>

```

### 1479 3.4.3 Kerberos

1480 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

1481 Note that this URI is also used as the target namespace in the corresponding authentication context class  
1482 schema document [SAMLAC-Kerb]).

1483 This class is defined for use when the Principal has authenticated using a password to a local  
1484 authentication authority, in order to acquire a Kerberos ticket. That Kerberos ticket is then used for  
1485 subsequent network authentication.

1486 **Note:** It is possible for the authentication authority to indicate (via this context class) a pre-  
1487 authentication data type which was used by the Kerberos Key Distribution Center [RFC 1510]  
1488 when authenticating the Principal. The method used by the authentication authority to obtain this  
1489 information is outside of the scope of this specification, but it is strongly recommended that a  
1490 trusted method be deployed to pass the pre-authentication data type and any other Kerberos  
1491 related context details (e.g. ticket lifetime) to the authentication authority.

```

1492 <xs:schema
1493 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1494 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1495 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
1496 finalDefault="extension">
1497

```

```

1498     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
1499     2.0.xsd">
1500
1501         <xs:annotation>
1502             <xs:documentation>
1503                 Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
1504                 Document identifier: sstc-saml-schema-authn-context-kerberos-2.0
1505                 Location: http://www.oasis-
1506 open.org/committees/documents.php?wg_abbrev=security
1507                 Revision history:
1508                     V2.0 CD-03 (December, 2004):
1509                     New authentication context class schema for SAML V2.0.
1510             </xs:documentation>
1511         </xs:annotation>
1512
1513         <xs:complexType name="AuthnContextDeclarationBaseType">
1514             <xs:complexContent>
1515                 <xs:restriction base="AuthnContextDeclarationBaseType">
1516                     <xs:sequence>
1517                         <xs:element ref="Identification" minOccurs="0"/>
1518                         <xs:element ref="TechnicalProtection" minOccurs="0"/>
1519                         <xs:element ref="OperationalProtection" minOccurs="0"/>
1520                         <xs:element ref="AuthnMethod"/>
1521                         <xs:element ref="GoverningAgreements" minOccurs="0"/>
1522                         <xs:element ref="Extension" minOccurs="0"
1523                             maxOccurs="unbounded"/>
1524                     </xs:sequence>
1525                     <xs:attribute name="ID" type="xs:ID"/>
1526                 </xs:restriction>
1527             </xs:complexContent>
1528         </xs:complexType>
1529
1530         <xs:complexType name="AuthnMethodBaseType">
1531             <xs:complexContent>
1532                 <xs:restriction base="AuthnMethodBaseType">
1533                     <xs:sequence>
1534                         <xs:element ref="PrincipalAuthenticationMechanism"/>
1535                         <xs:element ref="Authenticator"/>
1536                         <xs:element ref="AuthenticatorTransportProtocol"
1537                             minOccurs="0"/>
1538                         <xs:element ref="Extension" minOccurs="0"
1539                             maxOccurs="unbounded"/>
1540                     </xs:sequence>
1541                 </xs:restriction>
1542             </xs:complexContent>
1543         </xs:complexType>
1544
1545         <xs:complexType name="PrincipalAuthenticationMechanismType">
1546             <xs:complexContent>
1547                 <xs:restriction base="PrincipalAuthenticationMechanismType">
1548                     <xs:sequence>
1549                         <xs:choice>
1550                             <xs:element ref="RestrictedPassword"/>
1551                         </xs:choice>
1552                     </xs:sequence>
1553                     <xs:attribute name="preauth" type="xs:integer" use="optional"/>
1554                 </xs:restriction>
1555             </xs:complexContent>
1556         </xs:complexType>
1557
1558         <xs:complexType name="AuthenticatorBaseType">
1559             <xs:complexContent>
1560                 <xs:restriction base="AuthenticatorBaseType">
1561                     <xs:choice>
1562                         <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
1563                     </xs:choice>
1564                 </xs:restriction>

```

```

1565     </xs:complexContent>
1566 </xs:complexType>
1567
1568     <xs:complexType name="AuthenticatorSequenceType">
1569       <xs:complexContent>
1570         <xs:restriction base="AuthenticatorSequenceType">
1571           <xs:sequence>
1572             <xs:element ref="SharedSecretChallengeResponse"/>
1573           </xs:sequence>
1574         </xs:restriction>
1575       </xs:complexContent>
1576     </xs:complexType>
1577
1578     <xs:complexType name="SharedSecretChallengeResponseType">
1579       <xs:complexContent>
1580         <xs:restriction base="SharedSecretChallengeResponseType">
1581           <xs:attribute name="method" type="xs:anyURI"
1582 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos"/>
1583         </xs:restriction>
1584       </xs:complexContent>
1585     </xs:complexType>
1586
1587 </xs:redefine>
1588
1589 </xs:schema>

```

1590 An example of an XML instance conforming to this class schema is as follows:

```

1591 <AuthenticationContextDeclaration
1592   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1593   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos">
1594
1595   <AuthnMethod>
1596
1597     <PrincipalAuthenticationMechanism preauth="0">
1598       <RestrictedPassword>
1599         <Length min="4"/>
1600       </RestrictedPassword>
1601     </PrincipalAuthenticationMechanism>
1602
1603     <Authenticator>
1604       <AuthenticatorSequence>
1605         <SharedSecretChallengeResponse
1606 method="urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos"/>
1607       </AuthenticatorSequence>
1608     </Authenticator>
1609
1610   </AuthnMethod>
1611
1612 </AuthenticationContextDeclaration>

```

### 1613 3.4.4 MobileOneFactorUnregistered

1614 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered

1615 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 1616 schema document [SAMLAC-MOFU]).

1617 Reflects no mobile customer registration procedures and an authentication of the mobile device without  
 1618 requiring explicit end-user interaction. Again, this context authenticates only the device and never the  
 1619 user, it is useful when services other than the mobile operator want to add a secure device authentication  
 1620 to their authentication process.

```

1621 <xs:schema
1622 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUn
1623 registered"
1624 xmlns:xs="http://www.w3.org/2001/XMLSchema"

```

```

1625     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregister
1626 ed"
1627     finalDefault="extension">
1628
1629     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
1630 2.0.xsd">
1631
1632         <xs:annotation>
1633             <xs:documentation>
1634                 Class identifier:
1635                 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
1636                 Document identifier: sstc-saml-schema-authn-context-
1637                 mobileonefactor-unreg-2.0
1638                 Location: http://www.oasis-
1639                 open.org/committees/documents.php?wg_abbrev=security
1640                 Revision history:
1641                 V2.0 CD-03 (December, 2004):
1642                 New authentication context class schema for SAML V2.0.
1643             </xs:documentation>
1644         </xs:annotation>
1645
1646         <xs:complexType name="AuthnContextDeclarationBaseType">
1647             <xs:complexContent>
1648                 <xs:restriction base="AuthnContextDeclarationBaseType">
1649                     <xs:sequence>
1650                         <xs:element ref="Identification" minOccurs="0"/>
1651                         <xs:element ref="TechnicalProtection" minOccurs="0"/>
1652                         <xs:element ref="OperationalProtection" minOccurs="0"/>
1653                         <xs:element ref="AuthnMethod"/>
1654                         <xs:element ref="GoverningAgreements" minOccurs="0"/>
1655                         <xs:element ref="Extension" minOccurs="0"
1656                             maxOccurs="unbounded"/>
1657                     </xs:sequence>
1658                     <xs:attribute name="ID" type="xs:ID"/>
1659                 </xs:restriction>
1660             </xs:complexContent>
1661         </xs:complexType>
1662
1663         <xs:complexType name="AuthnMethodBaseType">
1664             <xs:complexContent>
1665                 <xs:restriction base="AuthnMethodBaseType">
1666                     <xs:sequence>
1667                         <xs:element ref="PrincipalAuthenticationMechanism"
1668                             minOccurs="0"/>
1669                         <xs:element ref="Authenticator"/>
1670                         <xs:element ref="AuthenticatorTransportProtocol"
1671                             minOccurs="0"/>
1672                         <xs:element ref="Extension" minOccurs="0"
1673                             maxOccurs="unbounded"/>
1674                     </xs:sequence>
1675                 </xs:restriction>
1676             </xs:complexContent>
1677         </xs:complexType>
1678
1679         <xs:complexType name="AuthenticatorBaseType">
1680             <xs:complexContent>
1681                 <xs:restriction base="AuthenticatorBaseType">
1682                     <xs:choice>
1683                         <xs:element ref="AuthenticatorChoice" minOccurs="1"/>
1684                     </xs:choice>
1685                 </xs:restriction>
1686             </xs:complexContent>
1687         </xs:complexType>
1688
1689         <xs:complexType name="AuthenticatorChoiceType">
1690             <xs:complexContent>
1691                 <xs:restriction base="AuthenticatorChoiceType">

```

```

1692         <xs:choice>
1693             <xs:element ref="DigSig"/>
1694             <xs:element ref="ZeroKnowledge"/>
1695             <xs:element ref="SharedSecretChallengeResponse"/>
1696             <xs:element ref="SharedSecretDynamicPlaintext"/>
1697             <xs:element ref="AsymmetricDecryption"/>
1698             <xs:element ref="AsymmetricKeyAgreement"/>
1699         </xs:choice>
1700     </xs:restriction>
1701 </xs:complexContent>
1702 </xs:complexType>
1703
1704 <xs:complexType name="AuthenticatorTransportProtocolType">
1705     <xs:complexContent>
1706         <xs:restriction base="AuthenticatorTransportProtocolType">
1707             <xs:choice>
1708                 <xs:element ref="SSL"/>
1709                 <xs:element ref="MobileNetworkRadioEncryption"/>
1710                 <xs:element ref="MobileNetworkEndToEndEncryption"/>
1711                 <xs:element ref="WTLS"/>
1712             </xs:choice>
1713         </xs:restriction>
1714     </xs:complexContent>
1715 </xs:complexType>
1716
1717 <xs:complexType name="OperationalProtectionType">
1718     <xs:complexContent>
1719         <xs:restriction base="OperationalProtectionType">
1720             <xs:sequence>
1721                 <xs:element ref="SecurityAudit"/>
1722                 <xs:element ref="DeactivationCallCenter"/>
1723                 <xs:element ref="Extension" minOccurs="0"
1724 maxOccurs="unbounded"/>
1725             </xs:sequence>
1726         </xs:restriction>
1727     </xs:complexContent>
1728 </xs:complexType>
1729
1730 <xs:complexType name="TechnicalProtectionBaseType">
1731     <xs:complexContent>
1732         <xs:restriction base="TechnicalProtectionBaseType">
1733             <xs:choice>
1734                 <xs:element ref="PrivateKeyProtection"/>
1735                 <xs:element ref="SecretKeyProtection"/>
1736             </xs:choice>
1737         </xs:restriction>
1738     </xs:complexContent>
1739 </xs:complexType>
1740
1741 <xs:complexType name="PrivateKeyProtectionType">
1742     <xs:complexContent>
1743         <xs:restriction base="PrivateKeyProtectionType">
1744             <xs:sequence>
1745                 <xs:element ref="KeyStorage"/>
1746                 <xs:element ref="Extension" minOccurs="0"
1747 maxOccurs="unbounded"/>
1748             </xs:sequence>
1749         </xs:restriction>
1750     </xs:complexContent>
1751 </xs:complexType>
1752
1753 <xs:complexType name="SecretKeyProtectionType">
1754     <xs:complexContent>
1755         <xs:restriction base="SecretKeyProtectionType">
1756             <xs:sequence>
1757                 <xs:element ref="KeyStorage"/>
1758                 <xs:element ref="Extension" minOccurs="0"

```

```

1759 maxOccurs="unbounded"/>
1760     </xs:sequence>
1761   </xs:restriction>
1762 </xs:complexContent>
1763 </xs:complexType>
1764
1765 <xs:complexType name="KeyStorageType">
1766   <xs:complexContent>
1767     <xs:restriction base="KeyStorageType">
1768       <xs:attribute name="medium" use="required">
1769         <xs:simpleType>
1770           <xs:restriction base="mediumType">
1771             <xs:enumeration value="MobileDevice"/>
1772             <xs:enumeration value="MobileAuthCard"/>
1773             <xs:enumeration value="smartcard"/>
1774           </xs:restriction>
1775         </xs:simpleType>
1776       </xs:attribute>
1777     </xs:restriction>
1778   </xs:complexContent>
1779 </xs:complexType>
1780
1781 <xs:complexType name="SecurityAuditType">
1782   <xs:complexContent>
1783     <xs:restriction base="SecurityAuditType">
1784       <xs:sequence>
1785         <xs:element ref="SwitchAudit"/>
1786         <xs:element ref="Extension" minOccurs="0"
1787 maxOccurs="unbounded"/>
1788       </xs:sequence>
1789     </xs:restriction>
1790   </xs:complexContent>
1791 </xs:complexType>
1792
1793 <xs:complexType name="IdentificationType">
1794   <xs:complexContent>
1795     <xs:restriction base="IdentificationType">
1796       <xs:sequence>
1797         <xs:element ref="GoverningAgreements"/>
1798         <xs:element ref="Extension" minOccurs="0"
1799 maxOccurs="unbounded"/>
1800       </xs:sequence>
1801       <xs:attribute name="nym">
1802         <xs:simpleType>
1803           <xs:restriction base="nymType">
1804             <xs:enumeration value="anonymity"/>
1805             <xs:enumeration value="pseudonymity"/>
1806           </xs:restriction>
1807         </xs:simpleType>
1808       </xs:attribute>
1809     </xs:restriction>
1810   </xs:complexContent>
1811 </xs:complexType>
1812
1813 </xs:redefine>
1814
1815 </xs:schema>

```

### 1816 3.4.5 MobileTwoFactorUnregistered

1817 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered

1818 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 1819 schema document [SAMLAC-MTFU]).

1820 Reflects no mobile customer registration procedures and a two-factor based authentication, such as



1821 secure device and user PIN. This context class is useful when a service other than the mobile operator  
1822 wants to link their customer ID to a mobile supplied two-factor authentication service by capturing mobile  
1823 phone data at enrollment.

```
1824 <?xml version="1.0" encoding="UTF-8"?>
1825
1826 <xs:schema
1827 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUn
1828 registered"
1829 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1830 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregister
1831 ed"
1832 finalDefault="extension">
1833
1834 <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
1835 2.0.xsd">
1836
1837 <xs:annotation>
1838 <xs:documentation>
1839 Class identifier:
1840 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
1841 Document identifier: sstc-saml-schema-authn-context-
1842 mobiletwofactor-unreg-2.0
1843 Location: http://www.oasis-
1844 open.org/committees/documents.php?wg_abbrev=security
1845 Revision history:
1846 V2.0 CD-03 (December, 2004):
1847 New authentication context class schema for SAML V2.0.
1848 </xs:documentation>
1849 </xs:annotation>
1850
1851 <xs:complexType name="AuthnContextDeclarationBaseType">
1852 <xs:complexContent>
1853 <xs:restriction base="AuthnContextDeclarationBaseType">
1854 <xs:sequence>
1855 <xs:element ref="Identification" minOccurs="0"/>
1856 <xs:element ref="TechnicalProtection" minOccurs="0"/>
1857 <xs:element ref="OperationalProtection" minOccurs="0"/>
1858 <xs:element ref="AuthnMethod"/>
1859 <xs:element ref="GoverningAgreements" minOccurs="0"/>
1860 <xs:element ref="Extension" minOccurs="0"
1861 maxOccurs="unbounded"/>
1862 </xs:sequence>
1863 <xs:attribute name="ID" type="xs:ID"/>
1864 </xs:restriction>
1865 </xs:complexContent>
1866 </xs:complexType>
1867
1868 <xs:complexType name="AuthnMethodBaseType">
1869 <xs:complexContent>
1870 <xs:restriction base="AuthnMethodBaseType">
1871 <xs:sequence>
1872 <xs:element ref="PrincipalAuthenticationMechanism"
1873 minOccurs="0"/>
1874 <xs:element ref="Authenticator"/>
1875 <xs:element ref="AuthenticatorTransportProtocol"
1876 minOccurs="0"/>
1877 <xs:element ref="Extension" minOccurs="0"
1878 maxOccurs="unbounded"/>
1879 </xs:sequence>
1880 </xs:restriction>
1881 </xs:complexContent>
1882 </xs:complexType>
1883
1884 <xs:complexType name="AuthenticatorBaseType">
1885 <xs:complexContent>
1886 <xs:restriction base="AuthenticatorBaseType">
```

```

1887         <xs:choice>
1888             <xs:element ref="AuthenticatorChoice" minOccurs="1"/>
1889         </xs:choice>
1890     </xs:restriction>
1891 </xs:complexContent>
1892 </xs:complexType>
1893
1894 <xs:complexType name="AuthenticatorChoiceType">
1895     <xs:complexContent>
1896         <xs:restriction base="AuthenticatorChoiceType">
1897             <xs:choice>
1898                 <xs:element ref="DigSig"/>
1899                 <xs:element ref="ZeroKnowledge"/>
1900                 <xs:element ref="SharedSecretChallengeResponse"/>
1901                 <xs:element ref="SharedSecretDynamicPlaintext"/>
1902                 <xs:element ref="AsymmetricDecryption"/>
1903                 <xs:element ref="AsymmetricKeyAgreement"/>
1904                 <xs:sequence>
1905                     <xs:element ref="Password" minOccurs="1"/>
1906                     <xs:choice>
1907                         <xs:element ref="SharedSecretDynamicPlaintext"/>
1908                         <xs:element ref="SharedSecretChallengeResponse"/>
1909                     </xs:choice>
1910                     <xs:element ref="Extension" maxOccurs="unbounded"/>
1911                 </xs:sequence>
1912             </xs:choice>
1913         </xs:restriction>
1914     </xs:complexContent>
1915 </xs:complexType>
1916
1917 <xs:complexType name="AuthenticatorTransportProtocolType">
1918     <xs:complexContent>
1919         <xs:restriction base="AuthenticatorTransportProtocolType">
1920             <xs:choice>
1921                 <xs:element ref="SSL"/>
1922                 <xs:element ref="MobileNetworkNoEncryption"/>
1923                 <xs:element ref="MobileNetworkRadioEncryption"/>
1924                 <xs:element ref="MobileNetworkEndToEndEncryption"/>
1925                 <xs:element ref="WTLS"/>
1926             </xs:choice>
1927         </xs:restriction>
1928     </xs:complexContent>
1929 </xs:complexType>
1930
1931 <xs:complexType name="OperationalProtectionType">
1932     <xs:complexContent>
1933         <xs:restriction base="OperationalProtectionType">
1934             <xs:sequence>
1935                 <xs:element ref="SecurityAudit"/>
1936                 <xs:element ref="DeactivationCallCenter"/>
1937                 <xs:element ref="Extension" minOccurs="0"
1938 maxOccurs="unbounded"/>
1939             </xs:sequence>
1940         </xs:restriction>
1941     </xs:complexContent>
1942 </xs:complexType>
1943
1944 <xs:complexType name="TechnicalProtectionBaseType">
1945     <xs:complexContent>
1946         <xs:restriction base="TechnicalProtectionBaseType">
1947             <xs:choice>
1948                 <xs:element ref="PrivateKeyProtection"/>
1949                 <xs:element ref="SecretKeyProtection"/>
1950             </xs:choice>
1951         </xs:restriction>
1952     </xs:complexContent>
1953 </xs:complexType>

```

1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020

```
<xs:complexType name="PrivateKeyProtectionType">
  <xs:complexContent>
    <xs:restriction base="PrivateKeyProtectionType">
      <xs:sequence>
        <xs:element ref="KeyActivation"/>
        <xs:element ref="KeyStorage"/>
        <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SecretKeyProtectionType">
  <xs:complexContent>
    <xs:restriction base="SecretKeyProtectionType">
      <xs:sequence>
        <xs:element ref="KeyActivation"/>
        <xs:element ref="KeyStorage"/>
        <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="KeyStorageType">
  <xs:complexContent>
    <xs:restriction base="KeyStorageType">
      <xs:attribute name="medium" use="required">
        <xs:simpleType>
          <xs:restriction base="mediumType">
            <xs:enumeration value="MobileDevice"/>
            <xs:enumeration value="MobileAuthCard"/>
            <xs:enumeration value="smartcard"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SecurityAuditType">
  <xs:complexContent>
    <xs:restriction base="SecurityAuditType">
      <xs:sequence>
        <xs:element ref="SwitchAudit"/>
        <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="IdentificationType">
  <xs:complexContent>
    <xs:restriction base="IdentificationType">
      <xs:sequence>
        <xs:element ref="GoverningAgreements"/>
        <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="nym">
        <xs:simpleType>
          <xs:restriction base="nymType">
            <xs:enumeration value="anonymity"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>
```

```

2021         <xs:enumeration value="pseudonymity"/>
2022         </xs:restriction>
2023         </xs:simpleType>
2024         </xs:attribute>
2025         </xs:restriction>
2026         </xs:complexContent>
2027     </xs:complexType>
2028
2029     </xs:redefine>
2030
2031 </xs:schema>

```

### 2032 3.4.6 MobileOneFactorContract

2033 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract

2034 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 2035 schema document [SAMLAC-MOFC]).

2036 Reflects mobile contract customer registration procedures and a single factor authentication. For example,  
 2037 a digital signing device with tamper resistant memory for key storage, such as the mobile MSISDN, but no  
 2038 required PIN or biometric for real-time user authentication.

```

2039 <xs:schema
2040 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorCo
2041 ntract"
2042   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2043   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
2044   finalDefault="extension">
2045
2046   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
2047 2.0.xsd">
2048
2049     <xs:annotation>
2050       <xs:documentation>
2051         Class identifier:
2052 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
2053         Document identifier: sstc-saml-schema-authn-context-
2054 mobileonefactor-reg-2.0
2055         Location: http://www.oasis-
2056 open.org/committees/documents.php?wg_abbrev=security
2057         Revision history:
2058           V2.0 CD-03 (December, 2004):
2059           New authentication context class schema for SAML V2.0.
2060       </xs:documentation>
2061     </xs:annotation>
2062
2063     <xs:complexType name="AuthnContextDeclarationBaseType">
2064       <xs:complexContent>
2065         <xs:restriction base="AuthnContextDeclarationBaseType">
2066           <xs:sequence>
2067             <xs:element ref="Identification" minOccurs="0"/>
2068             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2069             <xs:element ref="OperationalProtection" minOccurs="0"/>
2070             <xs:element ref="AuthnMethod"/>
2071             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2072             <xs:element ref="Extension" minOccurs="0"
2073               maxOccurs="unbounded"/>
2074           </xs:sequence>
2075           <xs:attribute name="ID" type="xs:ID"/>
2076         </xs:restriction>
2077       </xs:complexContent>
2078     </xs:complexType>
2079
2080     <xs:complexType name="AuthnMethodBaseType">
2081       <xs:complexContent>

```

```

2082     <xs:restriction base="AuthnMethodBaseType">
2083         <xs:sequence>
2084             <xs:element ref="PrincipalAuthenticationMechanism"
2085 minOccurs="0"/>
2086             <xs:element ref="Authenticator"/>
2087             <xs:element ref="AuthenticatorTransportProtocol"
2088                 minOccurs="0"/>
2089             <xs:element ref="Extension" minOccurs="0"
2090                 maxOccurs="unbounded"/>
2091         </xs:sequence>
2092     </xs:restriction>
2093 </xs:complexContent>
2094 </xs:complexType>
2095
2096 <xs:complexType name="AuthenticatorBaseType">
2097     <xs:complexContent>
2098         <xs:restriction base="AuthenticatorBaseType">
2099             <xs:choice>
2100                 <xs:element ref="AuthenticatorChoice" minOccurs="1"/>
2101             </xs:choice>
2102         </xs:restriction>
2103     </xs:complexContent>
2104 </xs:complexType>
2105
2106 <xs:complexType name="AuthenticatorChoiceType">
2107     <xs:complexContent>
2108         <xs:restriction base="AuthenticatorChoiceType">
2109             <xs:choice>
2110                 <xs:element ref="DigSig"/>
2111                 <xs:element ref="ZeroKnowledge"/>
2112                 <xs:element ref="SharedSecretChallengeResponse"/>
2113                 <xs:element ref="SharedSecretDynamicPlaintext"/>
2114                 <xs:element ref="AsymmetricDecryption"/>
2115                 <xs:element ref="AsymmetricKeyAgreement"/>
2116             </xs:choice>
2117         </xs:restriction>
2118     </xs:complexContent>
2119 </xs:complexType>
2120
2121 <xs:complexType name="AuthenticatorTransportProtocolType">
2122     <xs:complexContent>
2123         <xs:restriction base="AuthenticatorTransportProtocolType">
2124             <xs:choice>
2125                 <xs:element ref="SSL"/>
2126                 <xs:element ref="MobileNetworkNoEncryption"/>
2127                 <xs:element ref="MobileNetworkRadioEncryption"/>
2128                 <xs:element ref="MobileNetworkEndToEndEncryption"/>
2129                 <xs:element ref="WTLS"/>
2130             </xs:choice>
2131         </xs:restriction>
2132     </xs:complexContent>
2133 </xs:complexType>
2134
2135 <xs:complexType name="OperationalProtectionType">
2136     <xs:complexContent>
2137         <xs:restriction base="OperationalProtectionType">
2138             <xs:sequence>
2139                 <xs:element ref="SecurityAudit"/>
2140                 <xs:element ref="DeactivationCallCenter"/>
2141                 <xs:element ref="Extension" minOccurs="0"
2142 maxOccurs="unbounded"/>
2143             </xs:sequence>
2144         </xs:restriction>
2145     </xs:complexContent>
2146 </xs:complexType>
2147
2148 <xs:complexType name="TechnicalProtectionBaseType">

```

```

2149     <xs:complexContent>
2150       <xs:restriction base="TechnicalProtectionBaseType">
2151         <xs:choice>
2152           <xs:element ref="PrivateKeyProtection"/>
2153           <xs:element ref="SecretKeyProtection"/>
2154         </xs:choice>
2155       </xs:restriction>
2156     </xs:complexContent>
2157   </xs:complexType>
2158
2159   <xs:complexType name="PrivateKeyProtectionType">
2160     <xs:complexContent>
2161       <xs:restriction base="PrivateKeyProtectionType">
2162         <xs:sequence>
2163           <xs:element ref="KeyStorage"/>
2164           <xs:element ref="Extension" minOccurs="0"
2165 maxOccurs="unbounded"/>
2166         </xs:sequence>
2167       </xs:restriction>
2168     </xs:complexContent>
2169   </xs:complexType>
2170
2171   <xs:complexType name="SecretKeyProtectionType">
2172     <xs:complexContent>
2173       <xs:restriction base="SecretKeyProtectionType">
2174         <xs:sequence>
2175           <xs:element ref="KeyStorage"/>
2176           <xs:element ref="Extension" minOccurs="0"
2177 maxOccurs="unbounded"/>
2178         </xs:sequence>
2179       </xs:restriction>
2180     </xs:complexContent>
2181   </xs:complexType>
2182
2183   <xs:complexType name="KeyStorageType">
2184     <xs:complexContent>
2185       <xs:restriction base="KeyStorageType">
2186         <xs:attribute name="medium" use="required">
2187           <xs:simpleType>
2188             <xs:restriction base="mediumType">
2189               <xs:enumeration value="smartcard"/>
2190               <xs:enumeration value="MobileDevice"/>
2191               <xs:enumeration value="MobileAuthCard"/>
2192             </xs:restriction>
2193           </xs:simpleType>
2194         </xs:attribute>
2195       </xs:restriction>
2196     </xs:complexContent>
2197   </xs:complexType>
2198
2199   <xs:complexType name="SecurityAuditType">
2200     <xs:complexContent>
2201       <xs:restriction base="SecurityAuditType">
2202         <xs:sequence>
2203           <xs:element ref="SwitchAudit"/>
2204           <xs:element ref="Extension" minOccurs="0"
2205 maxOccurs="unbounded"/>
2206         </xs:sequence>
2207       </xs:restriction>
2208     </xs:complexContent>
2209   </xs:complexType>
2210
2211   <xs:complexType name="IdentificationType">
2212     <xs:complexContent>
2213       <xs:restriction base="IdentificationType">
2214         <xs:sequence>
2215           <xs:element ref="PhysicalVerification"/>

```

```

2216         <xs:element ref="WrittenConsent"/>
2217         <xs:element ref="GoverningAgreements"/>
2218         <xs:element ref="Extension" minOccurs="0"
2219 maxOccurs="unbounded"/>
2220     </xs:sequence>
2221     <xs:attribute name="nym">
2222         <xs:simpleType>
2223             <xs:restriction base="nymType">
2224                 <xs:enumeration value="anonymity"/>
2225                 <xs:enumeration value="verinymity"/>
2226                 <xs:enumeration value="pseudonymity"/>
2227             </xs:restriction>
2228         </xs:simpleType>
2229     </xs:attribute>
2230 </xs:restriction>
2231 </xs:complexContent>
2232 </xs:complexType>
2233
2234 </xs:redefine>
2235
2236 </xs:schema>

```

### 2237 3.4.7 MobileTwoFactorContract

2238 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract (

2239 Note that this URI is also used as the target namespace in the corresponding authentication context class  
2240 schema document [SAMLAC-MTFC]).

2241 Reflects mobile contract customer registration procedures and a two-factor based authentication. For  
2242 example, a digital signing device with tamper resistant memory for key storage, such as a GSM SIM, that  
2243 requires explicit proof of user identity and intent, such as a PIN or biometric.

```

2244 <xs:schema
2245 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorCo
2246 ntract"
2247   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2248   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
2249   finalDefault="extension">
2250
2251   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
2252 2.0.xsd">
2253
2254     <xs:annotation>
2255       <xs:documentation>
2256         Class identifier:
2257 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
2258         Document identifier: sstc-saml-schema-authn-context-
2259 mobiletwofactor-reg-2.0
2260         Location: http://www.oasis-
2261 open.org/committees/documents.php?wg_abbrev=security
2262         Revision history:
2263         V2.0 CD-03 (December, 2004):
2264         New authentication context class schema for SAML V2.0.
2265       </xs:documentation>
2266     </xs:annotation>
2267
2268     <xs:complexType name="AuthnContextDeclarationBaseType">
2269       <xs:complexContent>
2270         <xs:restriction base="AuthnContextDeclarationBaseType">
2271           <xs:sequence>
2272             <xs:element ref="Identification" minOccurs="0"/>
2273             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2274             <xs:element ref="OperationalProtection" minOccurs="0"/>
2275             <xs:element ref="AuthnMethod"/>
2276             <xs:element ref="GoverningAgreements" minOccurs="0"/>

```

```

2277         <xs:element ref="Extension" minOccurs="0"
2278             maxOccurs="unbounded"/>
2279     </xs:sequence>
2280     <xs:attribute name="ID" type="xs:ID"/>
2281 </xs:restriction>
2282 </xs:complexContent>
2283 </xs:complexType>
2284
2285 <xs:complexType name="AuthnMethodBaseType">
2286     <xs:complexContent>
2287         <xs:restriction base="AuthnMethodBaseType">
2288             <xs:sequence>
2289                 <xs:element ref="PrincipalAuthenticationMechanism"
2290 minOccurs="0"/>
2291                 <xs:element ref="Authenticator"/>
2292                 <xs:element ref="AuthenticatorTransportProtocol"
2293 minOccurs="0"/>
2294                 <xs:element ref="Extension" minOccurs="0"
2295 maxOccurs="unbounded"/>
2296             </xs:sequence>
2297         </xs:restriction>
2298     </xs:complexContent>
2299 </xs:complexType>
2300
2301 <xs:complexType name="AuthenticatorBaseType">
2302     <xs:complexContent>
2303         <xs:restriction base="AuthenticatorBaseType">
2304             <xs:choice>
2305                 <xs:element ref="AuthenticatorChoice" minOccurs="1"/>
2306             </xs:choice>
2307         </xs:restriction>
2308     </xs:complexContent>
2309 </xs:complexType>
2310
2311 <xs:complexType name="AuthenticatorChoiceType">
2312     <xs:complexContent>
2313         <xs:restriction base="AuthenticatorChoiceType">
2314             <xs:choice>
2315                 <xs:element ref="DigSig"/>
2316                 <xs:element ref="ZeroKnowledge"/>
2317                 <xs:element ref="SharedSecretChallengeResponse"/>
2318                 <xs:element ref="SharedSecretDynamicPlaintext"/>
2319                 <xs:element ref="AsymmetricDecryption"/>
2320                 <xs:element ref="AsymmetricKeyAgreement"/>
2321             <xs:sequence>
2322                 <xs:element ref="Password" minOccurs="1"/>
2323             <xs:choice>
2324                 <xs:element ref="SharedSecretDynamicPlaintext"/>
2325                 <xs:element ref="SharedSecretChallengeResponse"/>
2326             </xs:choice>
2327                 <xs:element ref="Extension" maxOccurs="unbounded"/>
2328             </xs:sequence>
2329         </xs:choice>
2330     </xs:restriction>
2331 </xs:complexContent>
2332 </xs:complexType>
2333
2334 <xs:complexType name="AuthenticatorTransportProtocolType">
2335     <xs:complexContent>
2336         <xs:restriction base="AuthenticatorTransportProtocolType">
2337             <xs:choice>
2338                 <xs:element ref="SSL"/>
2339                 <xs:element ref="MobileNetworkNoEncryption"/>
2340                 <xs:element ref="MobileNetworkRadioEncryption"/>
2341                 <xs:element ref="MobileNetworkEndToEndEncryption"/>
2342                 <xs:element ref="WTLS"/>
2343             </xs:choice>

```



```

2344     </xs:restriction>
2345     </xs:complexContent>
2346 </xs:complexType>
2347
2348 <xs:complexType name="OperationalProtectionType">
2349   <xs:complexContent>
2350     <xs:restriction base="OperationalProtectionType">
2351       <xs:sequence>
2352         <xs:element ref="SecurityAudit"/>
2353         <xs:element ref="DeactivationCallCenter"/>
2354         <xs:element ref="Extension" minOccurs="0"
2355 maxOccurs="unbounded"/>
2356       </xs:sequence>
2357     </xs:restriction>
2358   </xs:complexContent>
2359 </xs:complexType>
2360
2361 <xs:complexType name="TechnicalProtectionBaseType">
2362   <xs:complexContent>
2363     <xs:restriction base="TechnicalProtectionBaseType">
2364       <xs:choice>
2365         <xs:element ref="PrivateKeyProtection"/>
2366         <xs:element ref="SecretKeyProtection"/>
2367       </xs:choice>
2368     </xs:restriction>
2369   </xs:complexContent>
2370 </xs:complexType>
2371
2372 <xs:complexType name="PrivateKeyProtectionType">
2373   <xs:complexContent>
2374     <xs:restriction base="PrivateKeyProtectionType">
2375       <xs:sequence>
2376         <xs:element ref="KeyActivation"/>
2377         <xs:element ref="KeyStorage"/>
2378         <xs:element ref="Extension" minOccurs="0"
2379 maxOccurs="unbounded"/>
2380       </xs:sequence>
2381     </xs:restriction>
2382   </xs:complexContent>
2383 </xs:complexType>
2384
2385 <xs:complexType name="SecretKeyProtectionType">
2386   <xs:complexContent>
2387     <xs:restriction base="SecretKeyProtectionType">
2388       <xs:sequence>
2389         <xs:element ref="KeyActivation"/>
2390         <xs:element ref="KeyStorage"/>
2391         <xs:element ref="Extension" minOccurs="0"
2392 maxOccurs="unbounded"/>
2393       </xs:sequence>
2394     </xs:restriction>
2395   </xs:complexContent>
2396 </xs:complexType>
2397
2398 <xs:complexType name="KeyStorageType">
2399   <xs:complexContent>
2400     <xs:restriction base="KeyStorageType">
2401       <xs:attribute name="medium" use="required">
2402         <xs:simpleType>
2403           <xs:restriction base="mediumType">
2404             <xs:enumeration value="MobileDevice"/>
2405             <xs:enumeration value="MobileAuthCard"/>
2406             <xs:enumeration value="smartcard"/>
2407           </xs:restriction>
2408         </xs:simpleType>
2409       </xs:attribute>
2410     </xs:restriction>

```

```

2411     </xs:complexContent>
2412 </xs:complexType>
2413
2414     <xs:complexType name="SecurityAuditType">
2415       <xs:complexContent>
2416         <xs:restriction base="SecurityAuditType">
2417           <xs:sequence>
2418             <xs:element ref="SwitchAudit"/>
2419             <xs:element ref="Extension" minOccurs="0"
2420 maxOccurs="unbounded"/>
2421           </xs:sequence>
2422         </xs:restriction>
2423       </xs:complexContent>
2424     </xs:complexType>
2425
2426     <xs:complexType name="IdentificationType">
2427       <xs:complexContent>
2428         <xs:restriction base="IdentificationType">
2429           <xs:sequence>
2430             <xs:element ref="PhysicalVerification"/>
2431             <xs:element ref="WrittenConsent"/>
2432             <xs:element ref="GoverningAgreements"/>
2433             <xs:element ref="Extension" minOccurs="0"
2434 maxOccurs="unbounded"/>
2435           </xs:sequence>
2436           <xs:attribute name="nym">
2437             <xs:simpleType>
2438               <xs:restriction base="nymType">
2439                 <xs:enumeration value="anonymity"/>
2440                 <xs:enumeration value="verinymity"/>
2441                 <xs:enumeration value="pseudonymity"/>
2442               </xs:restriction>
2443             </xs:simpleType>
2444           </xs:attribute>
2445         </xs:restriction>
2446       </xs:complexContent>
2447     </xs:complexType>
2448 </xs:redefine>
2449
2450 </xs:schema>

```

### 2451 3.4.8 Password

2452 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Password

2453 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 2454 schema document [SAMLAC-Pass]).

2455 The Password class is identified when a Principal authenticates to an authentication authority through the  
 2456 presentation of a password over an unprotected HTTP session.

```

2457 <xs:schema
2458 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
2459 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2460 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
2461 finalDefault="extension">
2462
2463   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
2464 2.0.xsd">
2465
2466     <xs:annotation>
2467       <xs:documentation>
2468         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Password
2469         Document identifier: sstc-saml-schema-authn-context-pword-2.0
2470         Location: http://www.oasis-
2471 open.org/committees/documents.php?wg_abbrev=security

```

```

2472         Revision history:
2473             V2.0 CD-03 (December, 2004):
2474             New authentication context class schema for SAML V2.0.
2475         </xs:documentation>
2476     </xs:annotation>
2477
2478     <xs:complexType name="AuthnContextDeclarationBaseType">
2479         <xs:complexContent>
2480             <xs:restriction base="AuthnContextDeclarationBaseType">
2481                 <xs:sequence>
2482                     <xs:element ref="Identification" minOccurs="0"/>
2483                     <xs:element ref="TechnicalProtection" minOccurs="0"/>
2484                     <xs:element ref="OperationalProtection" minOccurs="0"/>
2485                     <xs:element ref="AuthnMethod" minOccurs="1"/>
2486                     <xs:element ref="GoverningAgreements" minOccurs="0"/>
2487                     <xs:element ref="Extension" minOccurs="0"
2488                         maxOccurs="unbounded"/>
2489                 </xs:sequence>
2490                 <xs:attribute name="ID" type="xs:ID"/>
2491             </xs:restriction>
2492         </xs:complexContent>
2493     </xs:complexType>
2494
2495     <xs:complexType name="AuthnMethodBaseType">
2496         <xs:complexContent>
2497             <xs:restriction base="AuthnMethodBaseType">
2498                 <xs:sequence>
2499                     <xs:element ref="PrincipalAuthenticationMechanism"
2500 minOccurs="0"/>
2501                     <xs:element ref="Authenticator" minOccurs="1"/>
2502                     <xs:element ref="AuthenticatorTransportProtocol"
2503                         minOccurs="0"/>
2504                     <xs:element ref="Extension" minOccurs="0"
2505                         maxOccurs="unbounded"/>
2506                 </xs:sequence>
2507             </xs:restriction>
2508         </xs:complexContent>
2509     </xs:complexType>
2510
2511     <xs:complexType name="AuthenticatorBaseType">
2512         <xs:complexContent>
2513             <xs:restriction base="AuthenticatorBaseType">
2514                 <xs:choice>
2515                     <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
2516                 </xs:choice>
2517             </xs:restriction>
2518         </xs:complexContent>
2519     </xs:complexType>
2520
2521     <xs:complexType name="AuthenticatorSequenceType">
2522         <xs:complexContent>
2523             <xs:restriction base="AuthenticatorSequenceType">
2524                 <xs:sequence>
2525                     <xs:element ref="RestrictedPassword"/>
2526                 </xs:sequence>
2527             </xs:restriction>
2528         </xs:complexContent>
2529     </xs:complexType>
2530
2531 </xs:redefine>
2532
2533 </xs:schema>

```

2534 Following is an example of an XML instance that conforms to the context class schema:

```

2535 <AuthenticationContextDeclaration
2536   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
2537   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password">
2538
2539   <AuthnMethod>
2540     <Authenticator>
2541       <AuthenticatorSequence>
2542         <RestrictedPassword>
2543           <Length min="4"/>
2544         </RestrictedPassword>
2545       </AuthenticatorSequence>
2546     </Authenticator>
2547   </AuthnMethod>
2548
2549 </AuthenticationContextDeclaration>

```

### 2550 3.4.9 PasswordProtectedTransport

2551 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

2552 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 2553 schema document [SAMLAC-PPT]).

2554 The PasswordProtectedTransport class is identified when a Principal authenticates to an authentication  
 2555 authority through the presentation of a password over a protected session.

```

2556 <xs:schema
2557 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected
2558 Transport"
2559   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2560   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
2561   finalDefault="extension">
2562
2563   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
2564 2.0.xsd">
2565
2566     <xs:annotation>
2567       <xs:documentation>
2568         Class identifier:
2569         urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
2570         Document identifier: sstc-saml-schema-authn-context-ppt-2.0
2571         Location: http://www.oasis-
2572 open.org/committees/documents.php?wg_abbrev=security
2573         Revision history:
2574         V2.0 CD-03 (December, 2004):
2575         New authentication context class schema for SAML V2.0.
2576       </xs:documentation>
2577     </xs:annotation>
2578
2579     <xs:complexType name="AuthnContextDeclarationBaseType">
2580       <xs:complexContent>
2581         <xs:restriction base="AuthnContextDeclarationBaseType">
2582           <xs:sequence>
2583             <xs:element ref="Identification" minOccurs="0"/>
2584             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2585             <xs:element ref="OperationalProtection" minOccurs="0"/>
2586             <xs:element ref="AuthnMethod"/>
2587             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2588             <xs:element ref="Extension" minOccurs="0"
2589               maxOccurs="unbounded"/>
2590           </xs:sequence>
2591           <xs:attribute name="ID" type="xs:ID"/>
2592         </xs:restriction>
2593       </xs:complexContent>
2594     </xs:complexType>
2595

```

```

2596
2597     <xs:complexType name="AuthnMethodBaseType">
2598       <xs:complexContent>
2599         <xs:restriction base="AuthnMethodBaseType">
2600           <xs:sequence>
2601             <xs:element ref="PrincipalAuthenticationMechanism"
2602 minOccurs="0"/>
2603             <xs:element ref="Authenticator"/>
2604             <xs:element ref="AuthenticatorTransportProtocol"/>
2605             <xs:element ref="Extension" minOccurs="0"
2606               maxOccurs="unbounded"/>
2607           </xs:sequence>
2608         </xs:restriction>
2609       </xs:complexContent>
2610     </xs:complexType>
2611
2612     <xs:complexType name="AuthenticatorBaseType">
2613       <xs:complexContent>
2614         <xs:restriction base="AuthenticatorBaseType">
2615           <xs:choice>
2616             <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
2617           </xs:choice>
2618         </xs:restriction>
2619       </xs:complexContent>
2620     </xs:complexType>
2621
2622     <xs:complexType name="AuthenticatorSequenceType">
2623       <xs:complexContent>
2624         <xs:restriction base="AuthenticatorSequenceType">
2625           <xs:sequence>
2626             <xs:element ref="RestrictedPassword"/>
2627           </xs:sequence>
2628         </xs:restriction>
2629       </xs:complexContent>
2630     </xs:complexType>
2631
2632     <xs:complexType name="AuthenticatorTransportProtocolType">
2633       <xs:complexContent>
2634         <xs:restriction base="AuthenticatorTransportProtocolType">
2635           <xs:choice>
2636             <xs:element ref="SSL"/>
2637             <xs:element ref="MobileNetworkRadioEncryption"/>
2638             <xs:element ref="MobileNetworkEndToEndEncryption"/>
2639             <xs:element ref="WTLS"/>
2640             <xs:element ref="IPSec"/>
2641           </xs:choice>
2642         </xs:restriction>
2643       </xs:complexContent>
2644     </xs:complexType>
2645
2646   </xs:redefine>
2647
2648 </xs:schema>

```

### 2649 **3.4.10 PreviousSession**

2650 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession

2651 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 2652 schema document [SAMLAC-Prev]).

2653 The PreviousSession class is identified when a Principal had authenticated to an authentication authority  
 2654 at some point in the past using any authentication context supported by that authentication authority.  
 2655 Consequently, a subsequent authentication event that the authentication authority will assert to the service  
 2656 provider may be significantly separated in time from the Principals current resource access request.

2657 The context for the previously authenticated session is explicitly not included in this context class because  
2658 the user has not authenticated during this session, and so the mechanism that the user employed to  
2659 authenticate in a previous session should not be used as part of a decision on whether to now allow  
2660 access to a resource.

```
2661 <xs:schema
2662 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2663 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2664 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
2665 finalDefault="extension">
2666
2667   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
2668 2.0.xsd">
2669
2670     <xs:annotation>
2671       <xs:documentation>
2672         Class identifier:
2673 urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
2674         Document identifier: sstc-saml-schema-authn-context-session-2.0
2675         Location: http://www.oasis-
2676 open.org/committees/documents.php?wg_abbrev=security
2677         Revision history:
2678           V2.0 CD-03 (December, 2004):
2679             New authentication context class schema for SAML V2.0.
2680       </xs:documentation>
2681     </xs:annotation>
2682
2683     <xs:complexType name="AuthnContextDeclarationBaseType">
2684       <xs:complexContent>
2685         <xs:restriction base="AuthnContextDeclarationBaseType">
2686           <xs:sequence>
2687             <xs:element ref="Identification" minOccurs="0"/>
2688             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2689             <xs:element ref="OperationalProtection" minOccurs="0"/>
2690             <xs:element ref="AuthnMethod"/>
2691             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2692             <xs:element ref="Extension" minOccurs="0"
2693               maxOccurs="unbounded"/>
2694           </xs:sequence>
2695           <xs:attribute name="ID" type="xs:ID"/>
2696         </xs:restriction>
2697       </xs:complexContent>
2698     </xs:complexType>
2699
2700     <xs:complexType name="AuthnMethodBaseType">
2701       <xs:complexContent>
2702         <xs:restriction base="AuthnMethodBaseType">
2703           <xs:sequence>
2704             <xs:element ref="PrincipalAuthenticationMechanism"
2705 minOccurs="0"/>
2706             <xs:element ref="Authenticator"/>
2707             <xs:element ref="AuthenticatorTransportProtocol"
2708               minOccurs="0"/>
2709             <xs:element ref="Extension" minOccurs="0"
2710               maxOccurs="unbounded"/>
2711           </xs:sequence>
2712         </xs:restriction>
2713       </xs:complexContent>
2714     </xs:complexType>
2715
2716     <xs:complexType name="AuthenticatorBaseType">
2717       <xs:complexContent>
2718         <xs:restriction base="AuthenticatorBaseType">
2719           <xs:choice>
2720             <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
2721           </xs:choice>
2722         </xs:restriction>

```

```

2723     </xs:complexContent>
2724 </xs:complexType>
2725
2726     <xs:complexType name="AuthenticatorSequenceType">
2727     <xs:complexContent>
2728     <xs:restriction base="AuthenticatorSequenceType">
2729     <xs:sequence>
2730     <xs:element ref="PreviousSession"/>
2731     </xs:sequence>
2732     </xs:restriction>
2733     </xs:complexContent>
2734 </xs:complexType>
2735
2736 </xs:redefine>
2737
2738 </xs:schema>

```

### 2739 3.4.11 Public Key – X.509

2740 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:X509

2741 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 2742 schema document [SAMLAC-X509]).

2743 The X509 context class indicates that the Principal authenticated by means of a digital signature where  
 2744 the key was validated as part of an X.509 Public Key Infrastructure.

```

2745 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2746   xmlns:xs="http://www.w3.org/2001/XMLSchema"
2747   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
2748   finalDefault="extension">
2749
2750   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
2751     2.0.xsd">
2752
2753     <xs:annotation>
2754     <xs:documentation>
2755     Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:X509
2756     Document identifier: sstc-saml-schema-authn-context-x509-2.0
2757     Location: http://www.oasis-
2758     open.org/committees/documents.php?wg_abbrev=security
2759     Revision history:
2760     V2.0 CD-03 (December, 2004):
2761     New authentication context class schema for SAML V2.0.
2762     </xs:documentation>
2763     </xs:annotation>
2764
2765     <xs:complexType name="AuthnContextDeclarationBaseType">
2766     <xs:complexContent>
2767     <xs:restriction base="AuthnContextDeclarationBaseType">
2768     <xs:sequence>
2769     <xs:element ref="Identification" minOccurs="0"/>
2770     <xs:element ref="TechnicalProtection" minOccurs="0"/>
2771     <xs:element ref="OperationalProtection" minOccurs="0"/>
2772     <xs:element ref="AuthnMethod"/>
2773     <xs:element ref="GoverningAgreements" minOccurs="0"/>
2774     <xs:element ref="Extension" minOccurs="0"
2775     maxOccurs="unbounded"/>
2776     </xs:sequence>
2777     <xs:attribute name="ID" type="xs:ID"/>
2778     </xs:restriction>
2779     </xs:complexContent>
2780     </xs:complexType>
2781
2782     <xs:complexType name="AuthnMethodBaseType">
2783     <xs:complexContent>

```

```

2784     <xs:restriction base="AuthnMethodBaseType">
2785         <xs:sequence>
2786             <xs:element ref="PrincipalAuthenticationMechanism"/>
2787             <xs:element ref="Authenticator"/>
2788             <xs:element ref="AuthenticatorTransportProtocol"
2789                 minOccurs="0"/>
2790             <xs:element ref="Extension" minOccurs="0"
2791                 maxOccurs="unbounded"/>
2792         </xs:sequence>
2793     </xs:restriction>
2794 </xs:complexContent>
2795 </xs:complexType>
2796
2797 <xs:complexType name="PrincipalAuthenticationMechanismType">
2798     <xs:complexContent>
2799         <xs:restriction base="PrincipalAuthenticationMechanismType">
2800             <xs:sequence>
2801                 <xs:choice>
2802                     <xs:element ref="RestrictedPassword"/>
2803                 </xs:choice>
2804             </xs:sequence>
2805             <xs:attribute name="preauth" type="xs:integer" use="optional"/>
2806         </xs:restriction>
2807     </xs:complexContent>
2808 </xs:complexType>
2809
2810 <xs:complexType name="AuthenticatorBaseType">
2811     <xs:complexContent>
2812         <xs:restriction base="AuthenticatorBaseType">
2813             <xs:choice>
2814                 <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
2815             </xs:choice>
2816         </xs:restriction>
2817     </xs:complexContent>
2818 </xs:complexType>
2819
2820 <xs:complexType name="AuthenticatorSequenceType">
2821     <xs:complexContent>
2822         <xs:restriction base="AuthenticatorSequenceType">
2823             <xs:sequence>
2824                 <xs:element ref="DigSig"/>
2825             </xs:sequence>
2826         </xs:restriction>
2827     </xs:complexContent>
2828 </xs:complexType>
2829
2830 <xs:complexType name="PublicKeyType">
2831     <xs:complexContent>
2832         <xs:restriction base="PublicKeyType">
2833             <xs:attribute name="keyValidation" type="xs:anyURI"
2834                 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
2835         </xs:restriction>
2836     </xs:complexContent>
2837 </xs:complexType>
2838
2839 </xs:redefine>
2840
2841 </xs:schema>

```

### 2842 **3.4.12 Public Key – PGP**

2843 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PGP

2844 Note that this URI is also used as the target namespace in the corresponding authentication context class  
2845 schema document [SAMLAC-PGP]).



2846 The PGP context class indicates that the Principal authenticated by means of a digital signature where the  
2847 key was validated as part of a PGP Public Key Infrastructure.

```
2848 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"  
2849   xmlns:xs="http://www.w3.org/2001/XMLSchema"  
2850   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"  
2851   finalDefault="extension">  
2852  
2853   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-  
2854     2.0.xsd">  
2855  
2856     <xs:annotation>  
2857       <xs:documentation>  
2858         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PGP  
2859         Document identifier: sstc-saml-schema-authn-context-pgp-2.0  
2860         Location: http://www.oasis-  
2861         open.org/committees/documents.php?wg_abbrev=security  
2862         Revision history:  
2863         V2.0 CD-03 (December, 2004):  
2864         New authentication context class schema for SAML V2.0.  
2865       </xs:documentation>  
2866     </xs:annotation>  
2867  
2868     <xs:complexType name="AuthnContextDeclarationBaseType">  
2869       <xs:complexContent>  
2870         <xs:restriction base="AuthnContextDeclarationBaseType">  
2871           <xs:sequence>  
2872             <xs:element ref="Identification" minOccurs="0"/>  
2873             <xs:element ref="TechnicalProtection" minOccurs="0"/>  
2874             <xs:element ref="OperationalProtection" minOccurs="0"/>  
2875             <xs:element ref="AuthnMethod"/>  
2876             <xs:element ref="GoverningAgreements" minOccurs="0"/>  
2877             <xs:element ref="Extension" minOccurs="0"  
2878               maxOccurs="unbounded"/>  
2879           </xs:sequence>  
2880           <xs:attribute name="ID" type="xs:ID"/>  
2881         </xs:restriction>  
2882       </xs:complexContent>  
2883     </xs:complexType>  
2884  
2885     <xs:complexType name="AuthnMethodBaseType">  
2886       <xs:complexContent>  
2887         <xs:restriction base="AuthnMethodBaseType">  
2888           <xs:sequence>  
2889             <xs:element ref="PrincipalAuthenticationMechanism"/>  
2890             <xs:element ref="Authenticator"/>  
2891             <xs:element ref="AuthenticatorTransportProtocol"  
2892               minOccurs="0"/>  
2893             <xs:element ref="Extension" minOccurs="0"  
2894               maxOccurs="unbounded"/>  
2895           </xs:sequence>  
2896         </xs:restriction>  
2897       </xs:complexContent>  
2898     </xs:complexType>  
2899  
2900     <xs:complexType name="PrincipalAuthenticationMechanismType">  
2901       <xs:complexContent>  
2902         <xs:restriction base="PrincipalAuthenticationMechanismType">  
2903           <xs:sequence>  
2904             <xs:choice>  
2905               <xs:element ref="RestrictedPassword"/>  
2906             </xs:choice>  
2907           </xs:sequence>  
2908           <xs:attribute name="preauth" type="xs:integer" use="optional"/>  
2909         </xs:restriction>  
2910       </xs:complexContent>  
2911     </xs:complexType>
```

```

2912
2913     <xs:complexType name="AuthenticatorBaseType">
2914         <xs:complexContent>
2915             <xs:restriction base="AuthenticatorBaseType">
2916                 <xs:choice>
2917                     <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
2918                 </xs:choice>
2919             </xs:restriction>
2920         </xs:complexContent>
2921     </xs:complexType>
2922
2923     <xs:complexType name="AuthenticatorSequenceType">
2924         <xs:complexContent>
2925             <xs:restriction base="AuthenticatorSequenceType">
2926                 <xs:sequence>
2927                     <xs:element ref="DigSig"/>
2928                 </xs:sequence>
2929             </xs:restriction>
2930         </xs:complexContent>
2931     </xs:complexType>
2932
2933     <xs:complexType name="PublicKeyType">
2934         <xs:complexContent>
2935             <xs:restriction base="PublicKeyType">
2936                 <xs:attribute name="keyValidation"
2937 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
2938             </xs:restriction>
2939         </xs:complexContent>
2940     </xs:complexType>
2941
2942 </xs:redefine>
2943
2944 </xs:schema>

```

### 2945 **3.4.13 Public Key – SPKI**

2946 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI

2947 Note that this URI is also used as the target namespace in the corresponding authentication context class  
 2948 schema document [SAMLAC-SPKI]).

2949 The SPKI context class indicates that the Principal authenticated by means of a digital signature where  
 2950 the key was validated via an SPKI Infrastructure.

```

2951 <xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2952 xmlns:xs="http://www.w3.org/2001/XMLSchema"
2953 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
2954 finalDefault="extension">
2955
2956   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
2957 2.0.xsd">
2958
2959     <xs:annotation>
2960       <xs:documentation>
2961         Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
2962         Document identifier: sstc-saml-schema-authn-context-spki-2.0
2963         Location: http://www.oasis-
2964 open.org/committees/documents.php?wg_abbrev=security
2965         Revision history:
2966           V2.0 CD-03 (December, 2004):
2967             New authentication context class schema for SAML V2.0.
2968       </xs:documentation>
2969     </xs:annotation>
2970
2971     <xs:complexType name="AuthnContextDeclarationBaseType">
2972       <xs:complexContent>

```

```

2973     <xs:restriction base="AuthnContextDeclarationBaseType">
2974         <xs:sequence>
2975             <xs:element ref="Identification" minOccurs="0"/>
2976             <xs:element ref="TechnicalProtection" minOccurs="0"/>
2977             <xs:element ref="OperationalProtection" minOccurs="0"/>
2978             <xs:element ref="AuthnMethod"/>
2979             <xs:element ref="GoverningAgreements" minOccurs="0"/>
2980             <xs:element ref="Extension" minOccurs="0"
2981                 maxOccurs="unbounded"/>
2982         </xs:sequence>
2983         <xs:attribute name="ID" type="xs:ID"/>
2984     </xs:restriction>
2985 </xs:complexContent>
2986 </xs:complexType>
2987
2988 <xs:complexType name="AuthnMethodBaseType">
2989     <xs:complexContent>
2990         <xs:restriction base="AuthnMethodBaseType">
2991             <xs:sequence>
2992                 <xs:element ref="PrincipalAuthenticationMechanism"/>
2993                 <xs:element ref="Authenticator"/>
2994                 <xs:element ref="AuthenticatorTransportProtocol"
2995                     minOccurs="0"/>
2996                 <xs:element ref="Extension" minOccurs="0"
2997                     maxOccurs="unbounded"/>
2998             </xs:sequence>
2999         </xs:restriction>
3000     </xs:complexContent>
3001 </xs:complexType>
3002
3003 <xs:complexType name="PrincipalAuthenticationMechanismType">
3004     <xs:complexContent>
3005         <xs:restriction base="PrincipalAuthenticationMechanismType">
3006             <xs:sequence>
3007                 <xs:choice>
3008                     <xs:element ref="RestrictedPassword"/>
3009                 </xs:choice>
3010             </xs:sequence>
3011             <xs:attribute name="preauth" type="xs:integer" use="optional"/>
3012         </xs:restriction>
3013     </xs:complexContent>
3014 </xs:complexType>
3015
3016 <xs:complexType name="AuthenticatorBaseType">
3017     <xs:complexContent>
3018         <xs:restriction base="AuthenticatorBaseType">
3019             <xs:choice>
3020                 <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
3021             </xs:choice>
3022         </xs:restriction>
3023     </xs:complexContent>
3024 </xs:complexType>
3025
3026 <xs:complexType name="AuthenticatorSequenceType">
3027     <xs:complexContent>
3028         <xs:restriction base="AuthenticatorSequenceType">
3029             <xs:sequence>
3030                 <xs:element ref="DigSig"/>
3031             </xs:sequence>
3032         </xs:restriction>
3033     </xs:complexContent>
3034 </xs:complexType>
3035
3036 <xs:complexType name="PublicKeyType">
3037     <xs:complexContent>
3038         <xs:restriction base="PublicKeyType">

```

```

3039         <xs:attribute name="keyValidation"
3040 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
3041     </xs:restriction>
3042     </xs:complexContent>
3043 </xs:complexType>
3044
3045     </xs:redefine>
3046
3047 </xs:schema>

```

### 3048 **3.4.14 Public Key - XML Digital Signature**

3049 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig

3050 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3051 schema document [SAMLAC-X509]).

3052 This context class indicates that the Principal authenticated by means of a digital signature according to  
3053 the processing rules specified in the XML Digital Signature specification [XMLSig].

```

3054 <xs:schema
3055 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
3056 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3057 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
3058 finalDefault="extension">
3059
3060     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
3061 2.0.xsd">
3062
3063         <xs:annotation>
3064             <xs:documentation>
3065                 Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
3066                 Document identifier: sstc-saml-schema-authn-context-xmlsig-2.0
3067                 Location: http://www.oasis-
3068 open.org/committees/documents.php?wg_abbrev=security
3069                 Revision history:
3070                 V2.0 CD-03 (December, 2004):
3071                 New authentication context class schema for SAML V2.0.
3072             </xs:documentation>
3073         </xs:annotation>
3074
3075         <xs:complexType name="AuthnContextDeclarationBaseType">
3076             <xs:complexContent>
3077                 <xs:restriction base="AuthnContextDeclarationBaseType">
3078                     <xs:sequence>
3079                         <xs:element ref="Identification" minOccurs="0"/>
3080                         <xs:element ref="TechnicalProtection" minOccurs="0"/>
3081                         <xs:element ref="OperationalProtection" minOccurs="0"/>
3082                         <xs:element ref="AuthnMethod"/>
3083                         <xs:element ref="GoverningAgreements" minOccurs="0"/>
3084                         <xs:element ref="Extension" minOccurs="0"
3085                             maxOccurs="unbounded"/>
3086                     </xs:sequence>
3087                     <xs:attribute name="ID" type="xs:ID"/>
3088                 </xs:restriction>
3089             </xs:complexContent>
3090         </xs:complexType>
3091
3092         <xs:complexType name="AuthnMethodBaseType">
3093             <xs:complexContent>
3094                 <xs:restriction base="AuthnMethodBaseType">
3095                     <xs:sequence>
3096                         <xs:element ref="PrincipalAuthenticationMechanism"/>
3097                         <xs:element ref="Authenticator"/>
3098                         <xs:element ref="AuthenticatorTransportProtocol"
3099                             minOccurs="0"/>

```

```

3100         <xs:element ref="Extension" minOccurs="0"
3101             maxOccurs="unbounded"/>
3102     </xs:sequence>
3103 </xs:restriction>
3104 </xs:complexContent>
3105 </xs:complexType>
3106
3107 <xs:complexType name="PrincipalAuthenticationMechanismType">
3108     <xs:complexContent>
3109         <xs:restriction base="PrincipalAuthenticationMechanismType">
3110             <xs:sequence>
3111                 <xs:choice>
3112                     <xs:element ref="RestrictedPassword"/>
3113                 </xs:choice>
3114             </xs:sequence>
3115             <xs:attribute name="preauth" type="xs:integer" use="optional"/>
3116         </xs:restriction>
3117     </xs:complexContent>
3118 </xs:complexType>
3119
3120 <xs:complexType name="AuthenticatorBaseType">
3121     <xs:complexContent>
3122         <xs:restriction base="AuthenticatorBaseType">
3123             <xs:choice>
3124                 <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
3125             </xs:choice>
3126         </xs:restriction>
3127     </xs:complexContent>
3128 </xs:complexType>
3129
3130 <xs:complexType name="AuthenticatorSequenceType">
3131     <xs:complexContent>
3132         <xs:restriction base="AuthenticatorSequenceType">
3133             <xs:sequence>
3134                 <xs:element ref="DigSig"/>
3135             </xs:sequence>
3136         </xs:restriction>
3137     </xs:complexContent>
3138 </xs:complexType>
3139
3140 <xs:complexType name="PublicKeyType">
3141     <xs:complexContent>
3142         <xs:restriction base="PublicKeyType">
3143             <xs:attribute name="keyValidation" type="xs:anyURI"
3144 fixed="urn:ietf:rfc:3075"/>
3145         </xs:restriction>
3146     </xs:complexContent>
3147 </xs:complexType>
3148
3149 </xs:redefine>
3150
3151 </xs:schema>

```

### 3152 3.4.15 Smartcard

3153 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard

3154 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3155 schema document [SAMLAC-Smart].

3156 The Smartcard class is identified when a Principal authenticates to an authentication authority using a  
3157 smartcard.

```

3158 <xs:schema
3159 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
3160 xmlns:xs="http://www.w3.org/2001/XMLSchema"

```

```

3161     xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
3162     finalDefault="extension">
3163
3164     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
3165     2.0.xsd">
3166
3167         <xs:annotation>
3168             <xs:documentation>
3169                 Class identifier:
3170                 urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
3171                 Document identifier: sstc-saml-schema-authn-context-smartcard-2.0
3172                 Location: http://www.oasis-
3173                 open.org/committees/documents.php?wg_abbrev=security
3174                 Revision history:
3175                 V2.0 CD-03 (December, 2004):
3176                 New authentication context class schema for SAML V2.0.
3177             </xs:documentation>
3178         </xs:annotation>
3179
3180         <xs:complexType name="AuthnContextDeclarationBaseType">
3181             <xs:complexContent>
3182                 <xs:restriction base="AuthnContextDeclarationBaseType">
3183                     <xs:sequence>
3184                         <xs:element ref="Identification" minOccurs="0"/>
3185                         <xs:element ref="TechnicalProtection" minOccurs="0"/>
3186                         <xs:element ref="OperationalProtection" minOccurs="0"/>
3187                         <xs:element ref="AuthnMethod"/>
3188                         <xs:element ref="GoverningAgreements" minOccurs="0"/>
3189                         <xs:element ref="Extension" minOccurs="0"
3190                             maxOccurs="unbounded"/>
3191                     </xs:sequence>
3192                     <xs:attribute name="ID" type="xs:ID"/>
3193                 </xs:restriction>
3194             </xs:complexContent>
3195         </xs:complexType>
3196
3197         <xs:complexType name="AuthnMethodBaseType">
3198             <xs:complexContent>
3199                 <xs:restriction base="AuthnMethodBaseType">
3200                     <xs:sequence>
3201                         <xs:element ref="PrincipalAuthenticationMechanism"/>
3202                         <xs:element ref="Authenticator"/>
3203                         <xs:element ref="AuthenticatorTransportProtocol"
3204                             minOccurs="0"/>
3205                         <xs:element ref="Extension" minOccurs="0"
3206                             maxOccurs="unbounded"/>
3207                     </xs:sequence>
3208                 </xs:restriction>
3209             </xs:complexContent>
3210         </xs:complexType>
3211
3212         <xs:complexType name="PrincipalAuthenticationMechanismType">
3213             <xs:complexContent>
3214                 <xs:restriction base="PrincipalAuthenticationMechanismType">
3215                     <xs:sequence>
3216                         <xs:choice>
3217                             <xs:element ref="Smartcard"/>
3218                         </xs:choice>
3219                     </xs:sequence>
3220                 </xs:restriction>
3221             </xs:complexContent>
3222         </xs:complexType>
3223     </xs:redefine>
3224 </xs:schema>
3225
3226

```

### 3227 3.4.16 SmartcardPKI

3228 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

3229 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3230 schema document [SAMLAC-SmPKI]).

3231 The SmartcardPKI class is identified when a Principal authenticates to an authentication authority through  
3232 a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN.

```
3233 <xs:schema
3234 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
3235 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3236 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
3237 finalDefault="extension">
3238
3239   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
3240 2.0.xsd">
3241
3242     <xs:annotation>
3243       <xs:documentation>
3244         Class identifier:
3245 urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
3246         Document identifier: sstc-saml-schema-authn-context-smartcardpki-
3247 2.0
3248         Location: http://www.oasis-
3249 open.org/committees/documents.php?wg_abbrev=security
3250         Revision history:
3251           V2.0 CD-03 (December, 2004):
3252           New authentication context class schema for SAML V2.0.
3253       </xs:documentation>
3254     </xs:annotation>
3255
3256     <xs:complexType name="AuthnContextDeclarationBaseType">
3257       <xs:complexContent>
3258         <xs:restriction base="AuthnContextDeclarationBaseType">
3259           <xs:sequence>
3260             <xs:element ref="Identification" minOccurs="0"/>
3261             <xs:element ref="TechnicalProtection"/>
3262             <xs:element ref="OperationalProtection" minOccurs="0"/>
3263             <xs:element ref="AuthnMethod"/>
3264             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3265             <xs:element ref="Extension" minOccurs="0"
3266               maxOccurs="unbounded"/>
3267           </xs:sequence>
3268           <xs:attribute name="ID" type="xs:ID"/>
3269         </xs:restriction>
3270       </xs:complexContent>
3271     </xs:complexType>
3272
3273     <xs:complexType name="AuthnMethodBaseType">
3274       <xs:complexContent>
3275         <xs:restriction base="AuthnMethodBaseType">
3276           <xs:sequence>
3277             <xs:element ref="PrincipalAuthenticationMechanism"/>
3278             <xs:element ref="Authenticator"/>
3279             <xs:element ref="AuthenticatorTransportProtocol"
3280               minOccurs="0"/>
3281             <xs:element ref="Extension" minOccurs="0"
3282               maxOccurs="unbounded"/>
3283           </xs:sequence>
3284         </xs:restriction>
3285       </xs:complexContent>
3286     </xs:complexType>
3287
3288     <xs:complexType name="TechnicalProtectionBaseType">
3289       <xs:complexContent>
```

```

3290     <xs:restriction base="TechnicalProtectionBaseType">
3291         <xs:sequence>
3292             <xs:choice>
3293                 <xs:element ref="PrivateKeyProtection"/>
3294             </xs:choice>
3295         </xs:sequence>
3296     </xs:restriction>
3297 </xs:complexContent>
3298 </xs:complexType>
3299
3300     <xs:complexType name="PrincipalAuthenticationMechanismType">
3301         <xs:complexContent>
3302             <xs:restriction base="PrincipalAuthenticationMechanismType">
3303                 <xs:sequence>
3304                     <xs:element ref="ActivationPin"/>
3305                     <xs:element ref="Smartcard"/>
3306                     <xs:element ref="Extension" minOccurs="0"
3307 maxOccurs="unbounded"/>
3308                 </xs:sequence>
3309             </xs:restriction>
3310         </xs:complexContent>
3311     </xs:complexType>
3312
3313     <xs:complexType name="AuthenticatorBaseType">
3314         <xs:complexContent>
3315             <xs:restriction base="AuthenticatorBaseType">
3316                 <xs:choice>
3317                     <xs:element ref="AuthenticatorChoice" minOccurs="1"/>
3318                 </xs:choice>
3319             </xs:restriction>
3320         </xs:complexContent>
3321     </xs:complexType>
3322
3323     <xs:complexType name="AuthenticatorChoiceType">
3324         <xs:complexContent>
3325             <xs:restriction base="AuthenticatorChoiceType">
3326                 <xs:choice>
3327                     <xs:element ref="DigSig"/>
3328                     <xs:element ref="AsymmetricDecryption"/>
3329                     <xs:element ref="AsymmetricKeyAgreement"/>
3330                 </xs:choice>
3331             </xs:restriction>
3332         </xs:complexContent>
3333     </xs:complexType>
3334
3335     <xs:complexType name="PrivateKeyProtectionType">
3336         <xs:complexContent>
3337             <xs:restriction base="PrivateKeyProtectionType">
3338                 <xs:sequence>
3339                     <xs:element ref="KeyActivation"/>
3340                     <xs:element ref="KeyStorage"/>
3341                     <xs:element ref="Extension" minOccurs="0"
3342 maxOccurs="unbounded"/>
3343                 </xs:sequence>
3344             </xs:restriction>
3345         </xs:complexContent>
3346     </xs:complexType>
3347
3348     <xs:complexType name="KeyActivationType">
3349         <xs:complexContent>
3350             <xs:restriction base="KeyActivationType">
3351                 <xs:choice>
3352                     <xs:element ref="ActivationPin"/>
3353                 </xs:choice>
3354             </xs:restriction>
3355         </xs:complexContent>
3356     </xs:complexType>

```



```

3357
3358     <xs:complexType name="KeyStorageType">
3359       <xs:complexContent>
3360         <xs:restriction base="KeyStorageType">
3361           <xs:attribute name="medium" use="required">
3362             <xs:simpleType>
3363               <xs:restriction base="mediumType">
3364                 <xs:enumeration value="smartcard"/>
3365               </xs:restriction>
3366             </xs:simpleType>
3367           </xs:attribute>
3368         </xs:restriction>
3369       </xs:complexContent>
3370     </xs:complexType>
3371
3372   </xs:redefine>
3373
3374 </xs:schema>

```

### 3375 3.4.17 SoftwarePKI

3376 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI

3377 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3378 schema document [SAMLAC-SwPKI] ).

3379 The Software-PKI class is identified when a Principal uses an X.509 certificate stored in software to  
3380 authenticate to the authentication authority.

```

3381 <xs:schema
3382 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3383 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3384 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
3385 finalDefault="extension">
3386
3387   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
3388 2.0.xsd">
3389
3390     <xs:annotation>
3391       <xs:documentation>
3392         Class identifier:
3393 urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
3394         Document identifier: sstc-saml-schema-authn-context-softwarepki-
3395 2.0
3396         Location: http://www.oasis-
3397 open.org/committees/documents.php?wg_abbrev=security
3398         Revision history:
3399           V2.0 CD-03 (December, 2004):
3400           New authentication context class schema for SAML V2.0.
3401       </xs:documentation>
3402     </xs:annotation>
3403
3404     <xs:complexType name="AuthnContextDeclarationBaseType">
3405       <xs:complexContent>
3406         <xs:restriction base="AuthnContextDeclarationBaseType">
3407           <xs:sequence>
3408             <xs:element ref="Identification" minOccurs="0"/>
3409             <xs:element ref="TechnicalProtection"/>
3410             <xs:element ref="OperationalProtection" minOccurs="0"/>
3411             <xs:element ref="AuthnMethod"/>
3412             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3413             <xs:element ref="Extension" minOccurs="0"
3414               maxOccurs="unbounded"/>
3415           </xs:sequence>
3416           <xs:attribute name="ID" type="xs:ID"/>
3417         </xs:restriction>

```

```

3418     </xs:complexContent>
3419 </xs:complexType>
3420
3421 <xs:complexType name="AuthnMethodBaseType">
3422   <xs:complexContent>
3423     <xs:restriction base="AuthnMethodBaseType">
3424       <xs:sequence>
3425         <xs:element ref="PrincipalAuthenticationMechanism"/>
3426         <xs:element ref="Authenticator"/>
3427         <xs:element ref="AuthenticatorTransportProtocol"
3428           minOccurs="0"/>
3429         <xs:element ref="Extension" minOccurs="0"
3430           maxOccurs="unbounded"/>
3431       </xs:sequence>
3432     </xs:restriction>
3433   </xs:complexContent>
3434 </xs:complexType>
3435
3436 <xs:complexType name="TechnicalProtectionBaseType">
3437   <xs:complexContent>
3438     <xs:restriction base="TechnicalProtectionBaseType">
3439       <xs:sequence>
3440         <xs:choice>
3441           <xs:element ref="PrivateKeyProtection"/>
3442         </xs:choice>
3443       </xs:sequence>
3444     </xs:restriction>
3445   </xs:complexContent>
3446 </xs:complexType>
3447
3448 <xs:complexType name="PrincipalAuthenticationMechanismType">
3449   <xs:complexContent>
3450     <xs:restriction base="PrincipalAuthenticationMechanismType">
3451       <xs:sequence>
3452         <xs:element ref="ActivationPin"/>
3453         <xs:element ref="Extension" minOccurs="0"
3454 maxOccurs="unbounded"/>
3455       </xs:sequence>
3456     </xs:restriction>
3457   </xs:complexContent>
3458 </xs:complexType>
3459
3460 <xs:complexType name="AuthenticatorBaseType">
3461   <xs:complexContent>
3462     <xs:restriction base="AuthenticatorBaseType">
3463       <xs:choice>
3464         <xs:element ref="AuthenticatorChoice" minOccurs="1"/>
3465       </xs:choice>
3466     </xs:restriction>
3467   </xs:complexContent>
3468 </xs:complexType>
3469
3470 <xs:complexType name="AuthenticatorChoiceType">
3471   <xs:complexContent>
3472     <xs:restriction base="AuthenticatorChoiceType">
3473       <xs:choice>
3474         <xs:element ref="DigSig"/>
3475         <xs:element ref="AsymmetricDecryption"/>
3476         <xs:element ref="AsymmetricKeyAgreement"/>
3477       </xs:choice>
3478     </xs:restriction>
3479   </xs:complexContent>
3480 </xs:complexType>
3481
3482 <xs:complexType name="PrivateKeyProtectionType">
3483   <xs:complexContent>
3484     <xs:restriction base="PrivateKeyProtectionType">

```

```

3485         <xs:sequence>
3486             <xs:element ref="KeyActivation"/>
3487             <xs:element ref="KeyStorage"/>
3488             <xs:element ref="Extension" minOccurs="0"
3489 maxOccurs="unbounded"/>
3490         </xs:sequence>
3491     </xs:restriction>
3492 </xs:complexContent>
3493 </xs:complexType>
3494
3495     <xs:complexType name="KeyActivationType">
3496         <xs:complexContent>
3497             <xs:restriction base="KeyActivationType">
3498                 <xs:choice>
3499                     <xs:element ref="ActivationPin"/>
3500                 </xs:choice>
3501             </xs:restriction>
3502 </xs:complexContent>
3503 </xs:complexType>
3504
3505     <xs:complexType name="KeyStorageType">
3506         <xs:complexContent>
3507             <xs:restriction base="KeyStorageType">
3508                 <xs:attribute name="medium" use="required">
3509                     <xs:simpleType>
3510                         <xs:restriction base="mediumType">
3511                             <xs:enumeration value="memory"/>
3512                         </xs:restriction>
3513                     </xs:simpleType>
3514                 </xs:attribute>
3515             </xs:restriction>
3516 </xs:complexContent>
3517 </xs:complexType>
3518
3519 </xs:redefine>
3520
3521 </xs:schema>

```

### 3522 3.4.18 Telephony

3523 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony

3524 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3525 schema document [SAMLAC-Tele].

3526 This class is used to indicate that the Principal authenticated via the provision of a fixed-line telephone  
3527 number, transported via a telephony protocol such as ADSL.

```

3528 <xs:schema
3529 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3530 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3531 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
3532 finalDefault="extension">
3533
3534     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
3535 2.0.xsd">
3536
3537         <xs:annotation>
3538             <xs:documentation>
3539                 Class identifier:
3540 urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
3541                 Document identifier: sstc-saml-schema-authn-context-telephony-2.0
3542                 Location: http://www.oasis-
3543 open.org/committees/documents.php?wg_abbrev=security
3544                 Revision history:
3545                 V2.0 CD-03 (December, 2004):

```

```

3546         New authentication context class schema for SAML V2.0.
3547     </xs:documentation>
3548 </xs:annotation>
3549
3550 <xs:complexType name="AuthnContextDeclarationBaseType">
3551     <xs:complexContent>
3552         <xs:restriction base="AuthnContextDeclarationBaseType">
3553             <xs:sequence>
3554                 <xs:element ref="Identification" minOccurs="0"/>
3555                 <xs:element ref="TechnicalProtection" minOccurs="0"/>
3556                 <xs:element ref="OperationalProtection" minOccurs="0"/>
3557                 <xs:element ref="AuthnMethod"/>
3558                 <xs:element ref="GoverningAgreements" minOccurs="0"/>
3559                 <xs:element ref="Extension" minOccurs="0"
3560                     maxOccurs="unbounded"/>
3561             </xs:sequence>
3562             <xs:attribute name="ID" type="xs:ID"/>
3563         </xs:restriction>
3564     </xs:complexContent>
3565 </xs:complexType>
3566
3567 <xs:complexType name="AuthnMethodBaseType">
3568     <xs:complexContent>
3569         <xs:restriction base="AuthnMethodBaseType">
3570             <xs:sequence>
3571                 <xs:element ref="PrincipalAuthenticationMechanism"
3572 minOccurs="0"/>
3573                 <xs:element ref="Authenticator"/>
3574                 <xs:element ref="AuthenticatorTransportProtocol"/>
3575                 <xs:element ref="Extension" minOccurs="0"
3576                     maxOccurs="unbounded"/>
3577             </xs:sequence>
3578         </xs:restriction>
3579     </xs:complexContent>
3580 </xs:complexType>
3581
3582 <xs:complexType name="AuthenticatorBaseType">
3583     <xs:complexContent>
3584         <xs:restriction base="AuthenticatorBaseType">
3585             <xs:choice>
3586                 <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
3587             </xs:choice>
3588         </xs:restriction>
3589     </xs:complexContent>
3590 </xs:complexType>
3591
3592 <xs:complexType name="AuthenticatorSequenceType">
3593     <xs:complexContent>
3594         <xs:restriction base="AuthenticatorSequenceType">
3595             <xs:sequence>
3596                 <xs:element ref="SubscriberLineNumber"/>
3597             </xs:sequence>
3598         </xs:restriction>
3599     </xs:complexContent>
3600 </xs:complexType>
3601
3602 <xs:complexType name="AuthenticatorTransportProtocolType">
3603     <xs:complexContent>
3604         <xs:restriction base="AuthenticatorTransportProtocolType">
3605             <xs:choice>
3606                 <xs:element ref="PSTN"/>
3607                 <xs:element ref="ISDN"/>
3608                 <xs:element ref="ADSL"/>
3609             </xs:choice>
3610         </xs:restriction>
3611     </xs:complexContent>
3612 </xs:complexType>

```

```
3613
3614     </xs:redefine>
3615
3616 </xs:schema>
```

### 3617 3.4.19 Telephony ("Nomadic")

3618 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony

3619 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3620 schema document [SAMLAC-TNom]).

3621 Indicates that the Principal is "roaming" (perhaps using a phone card) and authenticates via the means of  
3622 the line number, a user suffix, and a password element.

```
3623 <xs:schema
3624 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3625 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3626 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
3627 finalDefault="extension">
3628
3629   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
3630 2.0.xsd">
3631
3632     <xs:annotation>
3633       <xs:documentation>
3634         Class identifier:
3635 urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
3636         Document identifier: sstc-saml-schema-authn-context-nomad-
3637 telephony-2.0
3638         Location: http://www.oasis-
3639 open.org/committees/documents.php?wg_abbrev=security
3640         Revision history:
3641           V2.0 CD-03 (December, 2004):
3642             New authentication context class schema for SAML V2.0.
3643       </xs:documentation>
3644     </xs:annotation>
3645
3646     <xs:complexType name="AuthnContextDeclarationBaseType">
3647       <xs:complexContent>
3648         <xs:restriction base="AuthnContextDeclarationBaseType">
3649           <xs:sequence>
3650             <xs:element ref="Identification" minOccurs="0"/>
3651             <xs:element ref="TechnicalProtection" minOccurs="0"/>
3652             <xs:element ref="OperationalProtection" minOccurs="0"/>
3653             <xs:element ref="AuthnMethod"/>
3654             <xs:element ref="GoverningAgreements" minOccurs="0"/>
3655             <xs:element ref="Extension" minOccurs="0"
3656               maxOccurs="unbounded"/>
3657           </xs:sequence>
3658           <xs:attribute name="ID" type="xs:ID"/>
3659         </xs:restriction>
3660       </xs:complexContent>
3661     </xs:complexType>
3662
3663     <xs:complexType name="AuthnMethodBaseType">
3664       <xs:complexContent>
3665         <xs:restriction base="AuthnMethodBaseType">
3666           <xs:sequence>
3667             <xs:element ref="PrincipalAuthenticationMechanism"
3668 minOccurs="0"/>
3669             <xs:element ref="Authenticator"/>
3670             <xs:element ref="AuthenticatorTransportProtocol"/>
3671             <xs:element ref="Extension" minOccurs="0"
3672               maxOccurs="unbounded"/>
3673           </xs:sequence>
```

```

3674     </xs:restriction>
3675     </xs:complexContent>
3676 </xs:complexType>
3677
3678 <xs:complexType name="AuthenticatorBaseType">
3679   <xs:complexContent>
3680     <xs:restriction base="AuthenticatorBaseType">
3681       <xs:choice>
3682         <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
3683       </xs:choice>
3684     </xs:restriction>
3685   </xs:complexContent>
3686 </xs:complexType>
3687
3688 <xs:complexType name="AuthenticatorSequenceType">
3689   <xs:complexContent>
3690     <xs:restriction base="AuthenticatorSequenceType">
3691       <xs:sequence>
3692         <xs:element ref="Password"/>
3693         <xs:element ref="SubscriberLineNumber"/>
3694         <xs:element ref="UserSuffix"/>
3695       </xs:sequence>
3696     </xs:restriction>
3697   </xs:complexContent>
3698 </xs:complexType>
3699
3700 <xs:complexType name="AuthenticatorTransportProtocolType">
3701   <xs:complexContent>
3702     <xs:restriction base="AuthenticatorTransportProtocolType">
3703       <xs:choice>
3704         <xs:element ref="PSTN"/>
3705         <xs:element ref="ISDN"/>
3706         <xs:element ref="ADSL"/>
3707       </xs:choice>
3708     </xs:restriction>
3709   </xs:complexContent>
3710 </xs:complexType>
3711
3712 </xs:redefine>
3713
3714 </xs:schema>

```

### 3715 3.4.20 Telephony (Personalized)

3716 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony

3717 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3718 schema document [SAMLAC-TPers]).

3719 This class is used to indicate that the Principal authenticated via the provision of a fixed-line telephone  
3720 number and a user suffix, transported via a telephony protocol such as ADSL.

```

3721 <xs:schema
3722 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelep
3723 hony"
3724   xmlns:xs="http://www.w3.org/2001/XMLSchema"
3725   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
3726   finalDefault="extension">
3727
3728   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
3729 2.0.xsd">
3730
3731     <xs:annotation>
3732       <xs:documentation>
3733         Class identifier:
3734 urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony

```

```

3735         Document identifier: sstc-saml-schema-authn-context-personal-
3736 telephony-2.0
3737         Location: http://www.oasis-
3738 open.org/committees/documents.php?wg_abbrev=security
3739         Revision history:
3740             V2.0 CD-03 (December, 2004):
3741             New authentication context class schema for SAML V2.0.
3742         </xs:documentation>
3743     </xs:annotation>
3744
3745     <xs:complexType name="AuthnContextDeclarationBaseType">
3746         <xs:complexContent>
3747             <xs:restriction base="AuthnContextDeclarationBaseType">
3748                 <xs:sequence>
3749                     <xs:element ref="Identification" minOccurs="0"/>
3750                     <xs:element ref="TechnicalProtection" minOccurs="0"/>
3751                     <xs:element ref="OperationalProtection" minOccurs="0"/>
3752                     <xs:element ref="AuthnMethod"/>
3753                     <xs:element ref="GoverningAgreements" minOccurs="0"/>
3754                     <xs:element ref="Extension" minOccurs="0"
3755                         maxOccurs="unbounded"/>
3756                 </xs:sequence>
3757                 <xs:attribute name="ID" type="xs:ID"/>
3758             </xs:restriction>
3759         </xs:complexContent>
3760     </xs:complexType>
3761
3762     <xs:complexType name="AuthnMethodBaseType">
3763         <xs:complexContent>
3764             <xs:restriction base="AuthnMethodBaseType">
3765                 <xs:sequence>
3766                     <xs:element ref="PrincipalAuthenticationMechanism"
3767 minOccurs="0"/>
3768                     <xs:element ref="Authenticator"/>
3769                     <xs:element ref="AuthenticatorTransportProtocol"/>
3770                     <xs:element ref="Extension" minOccurs="0"
3771                         maxOccurs="unbounded"/>
3772                 </xs:sequence>
3773             </xs:restriction>
3774         </xs:complexContent>
3775     </xs:complexType>
3776
3777     <xs:complexType name="AuthenticatorBaseType">
3778         <xs:complexContent>
3779             <xs:restriction base="AuthenticatorBaseType">
3780                 <xs:choice>
3781                     <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
3782                 </xs:choice>
3783             </xs:restriction>
3784         </xs:complexContent>
3785     </xs:complexType>
3786
3787     <xs:complexType name="AuthenticatorSequenceType">
3788         <xs:complexContent>
3789             <xs:restriction base="AuthenticatorSequenceType">
3790                 <xs:sequence>
3791                     <xs:element ref="SubscriberLineNumber"/>
3792                     <xs:element ref="UserSuffix"/>
3793                 </xs:sequence>
3794             </xs:restriction>
3795         </xs:complexContent>
3796     </xs:complexType>
3797
3798     <xs:complexType name="AuthenticatorTransportProtocolType">
3799         <xs:complexContent>
3800             <xs:restriction base="AuthenticatorTransportProtocolType">
3801                 <xs:choice>

```

```

3802         <xs:element ref="PSTN"/>
3803         <xs:element ref="ISDN"/>
3804         <xs:element ref="ADSL"/>
3805     </xs:choice>
3806 </xs:restriction>
3807 </xs:complexContent>
3808 </xs:complexType>
3809
3810 </xs:redefine>
3811
3812 </xs:schema>

```

### 3813 3.4.21 Telephony (Authenticated)

3814 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony

3815 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3816 schema document [SAMLAC-TAuthn]).

3817 Indicates that the Principal authenticated via the means of the line number, a user suffix, and a password  
3818 element.

```

3819 <xs:schema
3820 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3821 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3822 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
3823 finalDefault="extension">
3824
3825     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-2.0.xsd">
3826
3827         <xs:annotation>
3828             <xs:documentation>
3829                 Class identifier:
3830                 urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
3831                 Document identifier: sstc-saml-schema-authn-context-auth-telephony-2.0
3832                 Location: http://www.oasis-open.org/committees/documents.php?wg_abbrev=security
3833                 Revision history:
3834                 V2.0 CD-03 (December, 2004):
3835                 New authentication context class schema for SAML V2.0.
3836             </xs:documentation>
3837         </xs:annotation>
3838
3839         <xs:complexType name="AuthnContextDeclarationBaseType">
3840             <xs:complexContent>
3841                 <xs:restriction base="AuthnContextDeclarationBaseType">
3842                     <xs:sequence>
3843                         <xs:element ref="Identification" minOccurs="0"/>
3844                         <xs:element ref="TechnicalProtection" minOccurs="0"/>
3845                         <xs:element ref="OperationalProtection" minOccurs="0"/>
3846                         <xs:element ref="AuthnMethod"/>
3847                         <xs:element ref="GoverningAgreements" minOccurs="0"/>
3848                         <xs:element ref="Extension" minOccurs="0"
3849                             maxOccurs="unbounded"/>
3850                     </xs:sequence>
3851                     <xs:attribute name="ID" type="xs:ID"/>
3852                 </xs:restriction>
3853             </xs:complexContent>
3854         </xs:complexType>
3855
3856         <xs:complexType name="AuthnMethodBaseType">
3857             <xs:complexContent>
3858                 <xs:restriction base="AuthnMethodBaseType">

```



```

3863         <xs:sequence>
3864             <xs:element ref="PrincipalAuthenticationMechanism"
3865 minOccurs="0"/>
3866             <xs:element ref="Authenticator"/>
3867             <xs:element ref="AuthenticatorTransportProtocol"/>
3868             <xs:element ref="Extension" minOccurs="0"
3869                 maxOccurs="unbounded"/>
3870         </xs:sequence>
3871     </xs:restriction>
3872 </xs:complexContent>
3873 </xs:complexType>
3874
3875 <xs:complexType name="AuthenticatorBaseType">
3876     <xs:complexContent>
3877         <xs:restriction base="AuthenticatorBaseType">
3878             <xs:choice>
3879                 <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
3880             </xs:choice>
3881         </xs:restriction>
3882     </xs:complexContent>
3883 </xs:complexType>
3884
3885 <xs:complexType name="AuthenticatorSequenceType">
3886     <xs:complexContent>
3887         <xs:restriction base="AuthenticatorSequenceType">
3888             <xs:sequence>
3889                 <xs:element ref="Password"/>
3890                 <xs:element ref="SubscriberLineNumber"/>
3891                 <xs:element ref="UserSuffix"/>
3892             </xs:sequence>
3893         </xs:restriction>
3894     </xs:complexContent>
3895 </xs:complexType>
3896
3897 <xs:complexType name="AuthenticatorTransportProtocolType">
3898     <xs:complexContent>
3899         <xs:restriction base="AuthenticatorTransportProtocolType">
3900             <xs:choice>
3901                 <xs:element ref="PSTN"/>
3902                 <xs:element ref="ISDN"/>
3903                 <xs:element ref="ADSL"/>
3904             </xs:choice>
3905         </xs:restriction>
3906     </xs:complexContent>
3907 </xs:complexType>
3908 </xs:redefine>
3909
3910 </xs:schema>

```

### 3911 **3.4.22 Secure Remote Password**

3912 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword

3913 Note that this URI is also used as the target namespace in the corresponding authentication context class  
3914 schema document [SAMLAC-SRP]).

3915 The Secure Remote Password class is indicated when the authentication was performed by means of  
3916 Secure Remote Password as specified in [RFC 2945].

```

3917 <xs:schema
3918 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassw
3919 ord"
3920 xmlns:xs="http://www.w3.org/2001/XMLSchema"
3921 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
3922 finalDefault="extension">
3923

```

```

3924     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
3925 2.0.xsd">
3926
3927         <xs:annotation>
3928             <xs:documentation>
3929                 Class identifier:
3930 urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
3931                 Document identifier: sstc-saml-schema-authn-context-srp-2.0
3932                 Location: http://www.oasis-
3933 open.org/committees/documents.php?wg_abbrev=security
3934                 Revision history:
3935                 V2.0 CD-03 (December, 2004):
3936                 New authentication context class schema for SAML V2.0.
3937             </xs:documentation>
3938         </xs:annotation>
3939
3940         <xs:complexType name="AuthnContextDeclarationBaseType">
3941             <xs:complexContent>
3942                 <xs:restriction base="AuthnContextDeclarationBaseType">
3943                     <xs:sequence>
3944                         <xs:element ref="Identification" minOccurs="0"/>
3945                         <xs:element ref="TechnicalProtection" minOccurs="0"/>
3946                         <xs:element ref="OperationalProtection" minOccurs="0"/>
3947                         <xs:element ref="AuthnMethod"/>
3948                         <xs:element ref="GoverningAgreements" minOccurs="0"/>
3949                         <xs:element ref="Extension" minOccurs="0"
3950                             maxOccurs="unbounded"/>
3951                     </xs:sequence>
3952                     <xs:attribute name="ID" type="xs:ID"/>
3953                 </xs:restriction>
3954             </xs:complexContent>
3955         </xs:complexType>
3956
3957         <xs:complexType name="AuthnMethodBaseType">
3958             <xs:complexContent>
3959                 <xs:restriction base="AuthnMethodBaseType">
3960                     <xs:sequence>
3961                         <xs:element ref="PrincipalAuthenticationMechanism"/>
3962                         <xs:element ref="Authenticator"/>
3963                         <xs:element ref="AuthenticatorTransportProtocol"
3964 minOccurs="0"/>
3965                         <xs:element ref="Extension" minOccurs="0"
3966                             maxOccurs="unbounded"/>
3967                     </xs:sequence>
3968                 </xs:restriction>
3969             </xs:complexContent>
3970         </xs:complexType>
3971
3972         <xs:complexType name="PrincipalAuthenticationMechanismType">
3973             <xs:complexContent>
3974                 <xs:restriction base="PrincipalAuthenticationMechanismType">
3975                     <xs:sequence>
3976                         <xs:choice>
3977                             <xs:element ref="RestrictedPassword"/>
3978                         </xs:choice>
3979                     </xs:sequence>
3980                 </xs:restriction>
3981             </xs:complexContent>
3982         </xs:complexType>
3983
3984         <xs:complexType name="AuthenticatorBaseType">
3985             <xs:complexContent>
3986                 <xs:restriction base="AuthenticatorBaseType">
3987                     <xs:choice>
3988                         <xs:element ref="AuthenticatorSequence" minOccurs="1"/>
3989                     </xs:choice>
3990                 </xs:restriction>

```

```

3991     </xs:complexContent>
3992 </xs:complexType>
3993
3994 <xs:complexType name="AuthenticatorSequenceType">
3995   <xs:complexContent>
3996     <xs:restriction base="AuthenticatorSequenceType">
3997       <xs:sequence>
3998         <xs:element ref="SharedSecretChallengeResponse"/>
3999       </xs:sequence>
4000     </xs:restriction>
4001   </xs:complexContent>
4002 </xs:complexType>
4003
4004 <xs:complexType name="SharedSecretChallengeResponseType">
4005   <xs:complexContent>
4006     <xs:restriction base="SharedSecretChallengeResponseType">
4007       <xs:attribute name="method" type="xs:anyURI"
4008 fixed="urn:ietf:rfc:2945"/>
4009     </xs:restriction>
4010   </xs:complexContent>
4011 </xs:complexType>
4012
4013 </xs:redefine>
4014
4015 </xs:schema>

```

### 4016 3.4.23 SSL/TLS Certificate-Based Client Authentication

4017 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient

4018 Note that this URI is also used as the target namespace in the corresponding authentication context class  
4019 schema document [SAMLAC-SSL].

4020 This class indicates that the Principal authenticated by means of a client certificate, secured with the  
4021 SSL/TLS transport.

```

4022 <?xml version="1.0" encoding="UTF-8"?>
4023
4024 <xs:schema
4025 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
4026 xmlns:xs="http://www.w3.org/2001/XMLSchema"
4027 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
4028 finalDefault="extension">
4029
4030   <xs:redefine schemaLocation="sstc-saml-schema-authn-context-
4031 types-2.0.xsd">
4032
4033     <xs:annotation>
4034       <xs:documentation>
4035         urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
4036       </xs:documentation>
4037     </xs:annotation>
4038
4039     <xs:complexType name="AuthnContextDeclarationBaseType">
4040       <xs:complexContent>
4041         <xs:restriction base="AuthnContextDeclarationBaseType">
4042           <xs:sequence>
4043             <xs:element ref="Identification" minOccurs="0"/>
4044             <xs:element ref="TechnicalProtection" minOccurs="0"/>
4045             <xs:element ref="OperationalProtection"
4046 minOccurs="0"/>
4047             <xs:element ref="AuthnMethod"/>
4048             <xs:element ref="GoverningAgreements" minOccurs="0"/>

```

```

4049         <xs:element ref="Extension" minOccurs="0"
4050             maxOccurs="unbounded"/>
4051     </xs:sequence>
4052     <xs:attribute name="ID" type="xs:ID"/>
4053 </xs:restriction>
4054 </xs:complexContent>
4055 </xs:complexType>
4056
4057 <xs:complexType name="AuthnMethodBaseType">
4058     <xs:complexContent>
4059         <xs:restriction base="AuthnMethodBaseType">
4060             <xs:sequence>
4061                 <xs:element ref="PrincipalAuthenticationMechanism"/>
4062                 <xs:element ref="Authenticator"/>
4063                 <xs:element ref="AuthenticatorTransportProtocol"
4064                     minOccurs="0"/>
4065                 <xs:element ref="Extension" minOccurs="0"
4066                     maxOccurs="unbounded"/>
4067             </xs:sequence>
4068         </xs:restriction>
4069     </xs:complexContent>
4070 </xs:complexType>
4071
4072 <xs:complexType name="PrincipalAuthenticationMechanismType">
4073     <xs:complexContent>
4074         <xs:restriction
4075 base="PrincipalAuthenticationMechanismType">
4076             <xs:sequence>
4077                 <xs:choice>
4078                     <xs:element ref="RestrictedPassword"/>
4079                 </xs:choice>
4080             </xs:sequence>
4081             <xs:attribute name="preauth" type="xs:integer"
4082 use="optional"/>
4083         </xs:restriction>
4084     </xs:complexContent>
4085 </xs:complexType>
4086
4087 <xs:complexType name="AuthenticatorBaseType">
4088     <xs:complexContent>
4089         <xs:restriction base="AuthenticatorBaseType">
4090             <xs:choice>
4091                 <xs:element ref="AuthenticatorSequence"
4092 minOccurs="1"/>
4093             </xs:choice>
4094         </xs:restriction>
4095     </xs:complexContent>
4096 </xs:complexType>
4097
4098 <xs:complexType name="AuthenticatorSequenceType">
4099     <xs:complexContent>
4100         <xs:restriction base="AuthenticatorSequenceType">
4101             <xs:sequence>
4102                 <xs:element ref="DigSig"/>
4103             </xs:sequence>
4104         </xs:restriction>
4105     </xs:complexContent>
4106 </xs:complexType>
4107
4108 <xs:complexType name="PublicKeyType">
4109     <xs:complexContent>

```

```

4110     <xs:restriction base="PublicKeyType">
4111         <xs:attribute name="keyValidation" type="xs:anyURI"
4112 fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
4113     </xs:restriction>
4114 </xs:complexContent>
4115 </xs:complexType>
4116
4117     <xs:complexType name="AuthenticatorTransportProtocolType">
4118     <xs:complexContent>
4119     <xs:restriction base="AuthenticatorTransportProtocolType">
4120     <xs:choice>
4121     <xs:element ref="SSL"/>
4122     <xs:element ref="WTLS"/>
4123     </xs:choice>
4124     </xs:restriction>
4125     </xs:complexContent>
4126 </xs:complexType>
4127
4128 </xs:redefine>
4129
4130 </xs:schema>

```

### 4131 3.4.24 TimeSyncToken

4132 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken

4133 Note that this URI is also used as the target namespace in the corresponding authentication context class  
4134 schema document [SAMLAC-TST]).

4135 The TimeSyncToken class is identified when a Principal authenticates through a time synchronization  
4136 token.

```

4137 <xs:schema
4138 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
4139 xmlns:xs="http://www.w3.org/2001/XMLSchema"
4140 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
4141 finalDefault="extension">
4142
4143     <xs:redefine schemaLocation="sstc-saml-schema-authn-context-types-
4144 2.0.xsd">
4145
4146     <xs:annotation>
4147     <xs:documentation>
4148     Class identifier:
4149 urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
4150 Document identifier: sstc-saml-schema-authn-context-timesync-2.0
4151 Location: http://www.oasis-
4152 open.org/committees/documents.php?wg_abbrev=security
4153 Revision history:
4154 V2.0 CD-03 (December, 2004):
4155 New authentication context class schema for SAML V2.0.
4156 </xs:documentation>
4157 </xs:annotation>
4158
4159     <xs:complexType name="AuthnContextDeclarationBaseType">
4160     <xs:complexContent>
4161     <xs:restriction base="AuthnContextDeclarationBaseType">
4162     <xs:sequence>
4163     <xs:element ref="Identification" minOccurs="0"/>
4164     <xs:element ref="TechnicalProtection" minOccurs="0"/>
4165     <xs:element ref="OperationalProtection" minOccurs="0"/>
4166     <xs:element ref="AuthnMethod"/>
4167     <xs:element ref="GoverningAgreements" minOccurs="0"/>
4168     <xs:element ref="Extension" minOccurs="0"

```

```

4169         maxOccurs="unbounded"/>
4170     </xs:sequence>
4171     <xs:attribute name="ID" type="xs:ID"/>
4172 </xs:restriction>
4173 </xs:complexContent>
4174 </xs:complexType>
4175
4176 <xs:complexType name="AuthnMethodBaseType">
4177     <xs:complexContent>
4178         <xs:restriction base="AuthnMethodBaseType">
4179             <xs:sequence>
4180                 <xs:element ref="PrincipalAuthenticationMechanism"
4181 minOccurs="0"/>
4182                 <xs:element ref="Authenticator"/>
4183                 <xs:element ref="AuthenticatorTransportProtocol"
4184 minOccurs="0"/>
4185                 <xs:element ref="Extension" minOccurs="0"
4186 maxOccurs="unbounded"/>
4187             </xs:sequence>
4188         </xs:restriction>
4189     </xs:complexContent>
4190 </xs:complexType>
4191
4192 <xs:complexType name="PrincipalAuthenticationMechanismType">
4193     <xs:complexContent>
4194         <xs:restriction base="PrincipalAuthenticationMechanismType">
4195             <xs:choice>
4196                 <xs:element ref="Token"/>
4197             </xs:choice>
4198         </xs:restriction>
4199     </xs:complexContent>
4200 </xs:complexType>
4201
4202 <xs:complexType name="TokenType">
4203     <xs:complexContent>
4204         <xs:restriction base="TokenType">
4205             <xs:sequence>
4206                 <xs:element ref="TimeSyncToken"/>
4207                 <xs:element ref="Extension" minOccurs="0"
4208 maxOccurs="unbounded"/>
4209             </xs:sequence>
4210         </xs:restriction>
4211     </xs:complexContent>
4212 </xs:complexType>
4213
4214 <xs:complexType name="TimeSyncTokenType">
4215     <xs:complexContent>
4216         <xs:restriction base="TimeSyncTokenType">
4217             <xs:attribute name="DeviceType" use="required">
4218                 <xs:simpleType>
4219                     <xs:restriction base="DeviceTypeType">
4220                         <xs:enumeration value="hardware"/>
4221                     </xs:restriction>
4222                 </xs:simpleType>
4223             </xs:attribute>
4224
4225             <xs:attribute name="SeedLength" use="required">
4226                 <xs:simpleType>
4227                     <xs:restriction base="xs:integer">
4228                         <xs:minInclusive value="64"/>
4229                     </xs:restriction>
4230                 </xs:simpleType>
4231             </xs:attribute>
4232
4233             <xs:attribute name="DeviceInHand" use="required">
4234                 <xs:simpleType>

```

```
4236         <xs:restriction base="booleanType">
4237             <xs:enumeration value="true"/>
4238         </xs:restriction>
4239     </xs:simpleType>
4240 </xs:attribute>
4241 </xs:restriction>
4242 </xs:complexContent>
4243 </xs:complexType>
4244
4245 </xs:redefine>
4246
4247 </xs:schema>
```

### 4248 **3.4.25 Unspecified**

4249 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

4250 The Unspecified class indicates that the authentication was performed by unspecified means.

---

## 4 References

4251

- 4252 [RFC 1510] J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5)*. IETF  
4253 RFC 1510, September 1993. <http://www.ietf.org/rfc/rfc1510.txt>.
- 4254 [RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
4255 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 4256 [RFC 2945] T. Wu. *The SRP Authentication and Key Exchange System*. IETF RFC 2945,  
4257 September 2000. <http://www.ietf.org/rfc/rfc2945.txt>.
- 4258 [SAMLAC-xsd] J. Kemp et al., SAML authentication context schema. OASIS SSTC, December  
4259 2004. Document ID sstc-saml-schema-authn-context-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)  
4260 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 4261 [SAMLACTypes] J. Kemp et al., SAML authentication context types schema. OASIS SSTC,  
4262 December 2004. Document ID sstc-saml-schema-authn-context-types-2.0. See  
4263 <http://www.oasis-open.org/committees/security/>.
- 4264 [SAMLAC-IP] J. Kemp et al., SAML context class schema for Internet Protocol. OASIS SSTC,  
4265 December 2004. Document ID sstc-saml-schema-authn-context-ip-2.0. See  
4266 <http://www.oasis-open.org/committees/security/>.
- 4267 [SAMLAC-IPP] J. Kemp et al., SAML context class schema for Internet Protocol Password.  
4268 OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-  
4269 ippassword-2.0. See <http://www.oasis-open.org/committees/security/>.
- 4270 [SAMLAC-Kerb] J. Kemp et al., SAML context class schema for Kerberos. OASIS SSTC,  
4271 December 2004. Document ID sstc-saml-schema-authn-context-kerberos-2.0.  
4272 See <http://www.oasis-open.org/committees/security/>.
- 4273 [SAMLAC-MOFC] J. Kemp et al., SAML context class schema for Mobile One Factor Contract.  
4274 Document ID sstc-saml-schema-authn-context-mobileonefactor-reg-2.0. See  
4275 OASIS SSTC, December 2004. <http://www.oasis-open.org/committees/security/>.
- 4276 [SAMLAC-MOFU] J. Kemp et al., SAML context class schema for Mobile One Factor Unregistered.  
4277 Document ID sstc-saml-schema-authn-context-mobileonefactor-unreg-2.0. See  
4278 OASIS SSTC, December 2004. <http://www.oasis-open.org/committees/security/>.
- 4279 [SAMLAC-MTFC] J. Kemp et al., SAML context class schema for Mobile Two Factor Contract.  
4280 OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-  
4281 mobiletwofactor-reg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 4282 [SAMLAC-MTFU] J. Kemp et al., SAML context class schema for Mobile Two Factor Unregistered.  
4283 OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-  
4284 mobiletwofactor-unreg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 4285 [SAMLAC-Pass] J. Kemp et al., SAML context class schema for Password. OASIS SSTC,  
4286 December 2004. Document ID sstc-saml-schema-authn-context-password-2.0. See  
4287 <http://www.oasis-open.org/committees/security/>.
- 4288 [SAMLAC-PGP] J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC,  
4289 December 2004. Document ID sstc-saml-schema-authn-context-pgp-2.0. See  
4290 <http://www.oasis-open.org/committees/security/>.
- 4291 [SAMLAC-PPT] J. Kemp et al., SAML context class schema for Password Protected Transport.  
4292 OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-  
4293 ppt-2.0. See <http://www.oasis-open.org/committees/security/>.
- 4294 [SAMLAC-Prev] J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC,  
4295 December 2004. Document ID sstc-saml-schema-authn-context-session-2.0. See  
4296 <http://www.oasis-open.org/committees/security/>.
- 4297 [SAMLAC-Smart] J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC,  
4298 December 2004. Document ID sstc-saml-schema-authn-context-smartcard-2.0.



4299		See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4300	<b>[SAMLAC-SmPKI]</b>	J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-smartcardpki-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4301		
4302		
4303	<b>[SAMLAC-SPKI]</b>	J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-spki-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4304		
4305		
4306	<b>[SAMLAC-SRP]</b>	J. Kemp et al., SAML context class schema for Secure Remote Password. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-srp-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4307		
4308		
4309	<b>[SAMLAC-SSL]</b>	J. Kemp et al., SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-sslcert-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4310		
4311		
4312	<b>[SAMLAC-SwPKI]</b>	J. Kemp et al., SAML context class schema for Software PKI. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-softwarepki-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4313		
4314		
4315	<b>[SAMLAC-Tele]</b>	J. Kemp et al., SAML context class schema for Telephony. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-telephony-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4316		
4317		
4318	<b>[SAMLAC-TNom]</b>	J. Kemp et al., SAML context class schema for Telephony (“Nomadic”). OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-nomad-telephony-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4319		
4320		
4321	<b>[SAMLAC-TPers]</b>	J. Kemp et al., SAML context class schema for Telephony (Personalized). OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-personal-telephony-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4322		
4323		
4324	<b>[SAMLAC-TAuthn]</b>	J. Kemp et al., SAML context class schema for Telephony (Authenticated). OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-auth-telephony-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4325		
4326		
4327	<b>[SAMLAC-TST]</b>	J. Kemp et al., SAML context class schema for Time Sync Token. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-timesync-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4328		
4329		
4330	<b>[SAMLAC-X509]</b>	J. Kemp et al., SAML context class schema for Public Key – X.509. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-x509-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4331		
4332		
4333	<b>[SAMLAC-XSig]</b>	J. Kemp et al., SAML context class schema for Public Key – XML Signature. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-xmldsig-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4334		
4335		
4336	<b>[SAMLCore]</b>	S. Cantor et al., <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, December 2004. Document ID sstc-saml-core-2.0-cd-03. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
4337		
4338		
4339	<b>[Schema1]</b>	H. S. Thompson et al. <i>XML Schema Part 1: Structures</i> . World Wide Web Consortium Recommendation, May 2001. <a href="http://www.w3.org/TR/xmlschema-1/">http://www.w3.org/TR/xmlschema-1/</a> .
4340		
4341	<b>[XMLSig]</b>	D. Eastlake et al., <i>XML-Signature Syntax and Processing</i> , World Wide Web Consortium, February 2002. <a href="http://www.w3.org/TR/xmldsig-core/">http://www.w3.org/TR/xmldsig-core/</a> .
4342		

---

## 4343 Appendix A. Acknowledgments

4344 The editors would like to acknowledge the contributions of the OASIS Security Services Technical  
4345 Committee, whose voting members at the time of publication were:

- 4346 • Conor Cahill, AOL
- 4347 • John Hughes, Atos Origin
- 4348 • Hal Lockhart, BEA Systems
- 4349 • Mike Beach, Boeing
- 4350 • Rebekah Metz, Booz Allen Hamilton
- 4351 • Rick Randall, Booz Allen Hamilton
- 4352 • Ronald Jacobson, Computer Associates
- 4353 • Paul Madsen, Entrust
- 4354 • Dana Kaufman, Forum Systems
- 4355 • Paula Austel, IBM
- 4356 • Michael McIntosh, IBM
- 4357 • Anthony Nadalin, IBM
- 4358 • Nick Ragouzis, Individual
- 4359 • Scott Cantor, Internet2
- 4360 • Bob Morgan, Internet2
- 4361 • Peter Davis, Neustar
- 4362 • Jeff Hodges, Neustar
- 4363 • Frederick Hirsch, Nokia
- 4364 • John Kemp, Nokia
- 4365 • Abbie Barbir, Nortel Networks
- 4366 • Scott Kiestler, Novell
- 4367 • Cameron Morris, Novell
- 4368 • Charles Knouse, Oblix
- 4369 • Steve Anderson, OpenNetwork
- 4370 • Ari Kermaier, Oracle
- 4371 • Vamsi Motukuru, Oracle
- 4372 • Darren Platt, Ping Identity
- 4373 • Prateek Mishra, Principal Identity
- 4374 • Jim Lien, RSA Security
- 4375 • Rob Philpott, RSA Security
- 4376 • Dipak Chopra, SAP
- 4377 • Jahan Moreh, Sigaba
- 4378 • Bhavna Bhatnagar, Sun Microsystems
- 4379 • Eve Maler, Sun Microsystems
- 4380 • Ronald Monzillo, Sun Microsystems
- 4381 • Emily Xu, Sun Microsystems
- 4382 • Greg Whitehead, Trustgenix
- 4383

4384

4385 The editors also would like to acknowledge the following people for their contributions to previous versions  
4386 of the OASIS Security Assertions Markup Language Standard:

- 4387 • Stephen Farrell, Baltimore Technologies
- 4388 • David Orchard, BEA Systems
- 4389 • Krishna Sankar, Cisco Systems
- 4390 • Zahid Ahmed, CommerceOne
- 4391 • Carlisle Adams, Entrust
- 4392 • Tim Moses, Entrust
- 4393 • Nigel Edwards, Hewlett-Packard
- 4394 • Joe Pato, Hewlett-Packard
- 4395 • Bob Blakley, IBM
- 4396 • Marlena Erdos, IBM
- 4397 • Marc Chanliau, Netegrity
- 4398 • Chris McLaren, Netegrity
- 4399 • Lynne Rosenthal, NIST
- 4400 • Mark Skall, NIST
- 4401 • Simon Godik, Overxeer
- 4402 • Charles Norwood, SAIC
- 4403 • Evan Prodromou, Securant
- 4404 • Robert Griffin, RSA Security (former editor)
- 4405 • Sai Allarvarpu, Sun Microsystems
- 4406 • Chris Ferris, Sun Microsystems
- 4407 • Emily Xu, Sun Microsystems
- 4408 • Mike Myers, Traceroute Security
- 4409 • Phillip Hallam-Baker, VeriSign (former editor)
- 4410 • James Vanderbeek, Vodafone
- 4411 • Mark O'Neill, Vordel
- 4412 • Tony Palmer, Vordel

4413

4414 Finally, the editors wish to acknowledge the following people for their contributions of material used as  
4415 input to the OASIS Security Assertions Markup Language specifications:

- 4416 • Thomas Gross, IBM
- 4417 • Birgit Pfitzmann, IBM

---

## 4418 Appendix B. Notices

4419 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that  
4420 might be claimed to pertain to the implementation or use of the technology described in this document or  
4421 the extent to which any license under such rights might or might not be available; neither does it represent  
4422 that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to  
4423 rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made  
4424 available for publication and any assurances of licenses to be made available, or the result of an attempt  
4425 made to obtain a general license or permission for the use of such proprietary rights by implementors or  
4426 users of this specification, can be obtained from the OASIS Executive Director.

4427 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or  
4428 other proprietary rights which may cover technology that may be required to implement this specification.  
4429 Please address the information to the OASIS Executive Director.

4430 **Copyright © OASIS Open 2004. All Rights Reserved.**

4431 This document and translations of it may be copied and furnished to others, and derivative works that  
4432 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and  
4433 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and  
4434 this paragraph are included on all such copies and derivative works. However, this document itself does  
4435 not be modified in any way, such as by removing the copyright notice or references to OASIS, except as  
4436 needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights  
4437 defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it  
4438 into languages other than English.

4439 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors  
4440 or assigns.

4441 This document and the information contained herein is provided on an "AS IS" basis and OASIS  
4442 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY  
4443 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR  
4444 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.