



Liberty ID-FF Authentication Context Specification

Version: 1.2

Editors:

Paul Madsen, Entrust Inc

Contributors:

Robert Aarts, Nokia

Nick Bone, Vodafone

Scott Cantor, OSU/Internet2

Slava Kavsan, RSA Security

John Kemp, IEEE-ISTO

Mike Meyerstein, Vodafone

Xavier Serret, Gemplus

Abstract:

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

Filename: liberty-authentication-context-v1.2.pdf

1 Notice

2 Copyright © 2003 America Online, Inc.; American Express Travel Related Services; Bank of America; Bell Canada;
3 Cingular Wireless; Cisco Systems, Inc.; Communicator, Inc.; Deloitte & Touche LLP; Earthlink, Inc.; Electronic
4 Data Systems, Inc.; Entrust, Inc.; Ericsson; Fidelity Investments; France Telecom; Gemplus; General Motors;
5 Hewlett-Packard Company; i2 Technologies, Inc.; Intuit Inc.; MasterCard International; NEC Corporation; Netegrity;
6 NeuStar; Nextel Communications; Nippon Telegraph and Telephone Corporation; Nokia Corporation; Novell, Inc.;
7 NTT DoCoMo, Inc.; OneName Corporation; Openwave Systems Inc.; PricewaterhouseCoopers LLP; Register.com;
8 Royal Mail; RSA Security Inc; Sabre Holdings Corporation; SAP AG; SchlumbergerSema; SK Telecom; Sony
9 Corporation; Sun Microsystems, Inc.; Symlabs, Inc.; Trustgenix; United Airlines; VeriSign, Inc.; Visa International;
10 Vodafone Group Plc; Wave Systems;. All rights reserved.

11 This specification document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to
12 use the document solely for the purpose of implementing the Specification. No rights are granted to prepare
13 derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other
14 uses must contact the Liberty Alliance to determine whether an appropriate license for such use is available.

15 Implementation of certain elements of this Specification may require licenses under third party intellectual property
16 rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are
17 not, and shall not be held responsible in any manner, for identifying or failing to identify any or all such third party
18 intellectual property rights. **This Specification is provided "AS IS", and no participant in the Liberty Alliance**
19 **makes any warranty of any kind, express or implied, including any implied warranties of merchantability,**
20 **non-infringement of third party intellectual property rights, and fitness for a particular purpose.** Implementors
21 of this Specification are advised to review the Liberty Alliance Project's website (<http://www.projectliberty.org/>) for
22 information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance
23 Management Board.

24 Liberty Alliance Project
25 Licensing Administrator
26 c/o IEEE-ISTO
27 445 Hoes Lane
28 Piscataway, NJ 08855-1331, USA
29 info@projectliberty.org

30 **Contents**

31	1. About this Document	4
32	2. Overview	5
33	3. Authentication Context	6
34	4. Authentication Context Statement	7
35	5. Authentication Context Classes	19
36	References	39

37 1. About this Document

38 This specification defines a syntax for the definition of authentication context statements and an initial list of Liberty
39 authentication context classes.

40 1.1. Notation and Terminology

41 This section specifies the notations, namespaces and terminology used throughout this specification. This
42 specification uses schema documents conforming to W3C XML Schema (see [Schema1]) and normative text to
43 describe the syntax and semantics of XML-encoded messages.

44 1.1.1. Notational Conventions

45 Note: Phrases and numbers in brackets [] refer to other documents; details of these references can be found in Section
46 3(at the end of this document).

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

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

52 Listings of XML schemas appear like this.

53 Example code listings appear like this.

54 1.1.2. Namespaces

55 The following namespaces are referred to in this document:

56 Table 1. Namespaces

Prefix	Namespace
ac	urn:liberty:ac:1.2
lib	urn:liberty:iff:1.2
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

57 This specification uses the following typographical conventions in text: <Element>, <ns:ForeignElement>, Attribute,
58 Datatype, OtherCode.

59 2. Overview

60 Liberty will not prescribe a single technology, protocol, or policy for the processes by which identity providers issue
61 identities to Principals and by which those Principals subsequently authenticate themselves to the identity provider.
62 Different identity providers will choose different technologies, follow different processes, and be bound by different
63 legal obligations with respect to how they authenticate Principals.

64 The choices that an identity provider makes here will be driven in large part by the requirements of the service providers
65 with which the identity provider has affiliated into a circle of trust. These requirements themselves will be determined
66 by the nature of the service (that is, the sensitivity of any information exchanged, the associated financial value, the
67 service providers risk tolerance, etc.) that the service provider will be providing to the Principal.

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

74 *Authentication context* is defined as the information, additional to the authentication assertion itself, that the service
75 provider may require before it makes an entitlements decision with respect to an authentication assertion.

76 **3. Authentication Context**

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

- 80 • What were the initial user identification mechanisms (for example, face-to-face, online, shared secret.
- 81 • What are the mechanisms for minimizing compromise of credentials (for example, credential renewal frequency,
82 client-side key generation).
- 83 • What are the mechanisms for storing and protecting credentials (for example, smartcard, password rules).
- 84 • What was the authentication mechanism (for example, password, certificate-based SSL).

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

88 4. Authentication Context Statement

89 A Liberty authentication authority will deliver to a relying party the additional authentication context information
90 in the form of an Authentication Context Statement, an XML document either inserted or referenced within the
91 <AuthnResponse> message the authentication authority returns to the relying party.

92 4.1. Authentication Context Statement Data Model

93 A particular Liberty authentication context statement will capture the characteristics of the processes, procedures,
94 and mechanisms by which the authentication verified the subject before issuing an identity, protects the secrets on
95 which subsequent authentications are based, and the mechanisms used for this authentication. These characteristics
96 are categorized in the Liberty Authentication Context schema as follows:

- 97 • Identification - Characteristics that describe the processes and mechanism the authentication authority uses to
98 initially create an association between a subject and the identity (or name) by which the subject will be known.
- 99 • Technical Protection - Characteristics that describe how the "secret" (the knowledge or possession of which allows
100 the subject to authenticate to the authentication authority) is kept secure.
- 101 • Operational Protection - Characteristics that describe procedural security controls employed by the authentication
102 authority (for example, security audits, records archival).
- 103 • Authentication Method - Characteristics that define the mechanisms by which the subject of the issued assertion
104 authenticates to the authentication authority (for example, a password versus a smartcard).
- 105 • Governing Agreements - Characteristics that describe the legal framework (e.g. liability constraints and contractual
106 obligations) underlying the authentication event and/or its associated technical authentication infrastructure.

107 4.2. Authentication Context Statement Schema

108 This section lists the complete Authentication Context XML Schema.

```
109
110 <?xml version="1.0" encoding="UTF-8"?>
111 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
112   xmlns:xs="http://www.w3.org/2001/XMLSchema"
113   xmlns="urn:liberty:ac:2003-08">
114
115   <!-- added to get the Extension element -->
116   <xs:include schemaLocation="liberty-utility-v1.0.xsd"/>
117
118   <xs:annotation>
119     <xs:documentation> ### IMPORTANT NOTICE ###
120
121     The source code in this XSD file was excerpted verbatim from:
122
123     Liberty Authentication Context Specification
124     Version 1.2
125     12 November 2003
126
127     Copyright (c) 2003 Liberty Alliance participants, see
128     http://www.projectliberty.org/specs/idf_copyrights.html
129   </xs:documentation>
130 </xs:annotation>
131 <xs:element name="AuthenticationContextStatement" type="AuthenticationContextStatementType">
132   <xs:annotation>
133     <xs:documentation>
134       A particular assertion on an identity
135       provider's part with respect to the authentication
```

```

136         context associated with an authentication assertion.
137     </xs:documentation>
138 </xs:annotation>
139 </xs:element>
140 <xs:element name="Identification" type="IdentificationType">
141     <xs:annotation>
142         <xs:documentation>
143             Refers to those characteristics that describe the processes and mechanisms
144             the Authentication Authority uses to initially create an association between a Principal
145             and the identity (or name) by which the Principal will be known
146         </xs:documentation>
147     </xs:annotation>
148 </xs:element>
149 <xs:element name="PhysicalVerification">
150     <xs:annotation>
151         <xs:documentation>
152             This element indicates that identification has been performed in a physical
153             face-to-face meeting with the principal and not in an online manner.
154         </xs:documentation>
155     </xs:annotation>
156     <xs:complexType>
157         <xs:attribute name="credentialLevel">
158             <xs:simpleType>
159                 <xs:restriction base="xs:NMTOKEN">
160                     <xs:enumeration value="primary"/>
161                     <xs:enumeration value="secondary"/>
162                 </xs:restriction>
163             </xs:simpleType>
164         </xs:attribute>
165     </xs:complexType>
166 </xs:element>
167 <xs:element name="WrittenConsent">
168     <xs:complexType>
169         <xs:sequence>
170             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
171         </xs:sequence>
172     </xs:complexType>
173 </xs:element>
174 <xs:element name="TechnicalProtection" type="TechnicalProtectionType">
175     <xs:annotation>
176         <xs:documentation>
177             Refers to those characteristics that describe how the 'secret' (the knowledge or
178 possession
179 of which allows the Principal to authenticate to the Authentication Authority) is kept
180 t secure
181         </xs:documentation>
182     </xs:annotation>
183 </xs:element>
184 <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType">
185     <xs:annotation>
186         <xs:documentation>
187             This element indicates the types and strengths of facilities
188             of a UA used to protect a shared secret key from unauthorized access and/or use.
189         </xs:documentation>
190     </xs:annotation>
191 </xs:element>
192 <xs:element name="PrivateKeyProtection" type="PrivateKeyProtectionType">
193     <xs:annotation>
194         <xs:documentation>
195             This element indicates the types and strengths of facilities
196             of a UA used to protect a private key from unauthorized access and/or use.
197         </xs:documentation>
198     </xs:annotation>
199 </xs:element>
200 <xs:element name="KeyActivation" type="KeyActivationType">
201     <xs:annotation>
202         <xs:documentation>The actions that must be performed before the private key can be used.
  
```



```

203 </xs:documentation>
204   </xs:annotation>
205 </xs:element>
206 <xs:element name="KeySharing" type="KeySharingType">
207   <xs:annotation>
208     <xs:documentation>Whether or not the private key is shared with the certificate_
209 authority.</xs:documentation>
210   </xs:annotation>
211 </xs:element>
212 <xs:element name="KeyStorage" type="KeyStorageType">
213   <xs:annotation>
214     <xs:documentation>
215       In which medium is the key stored.
216       memory - the key is stored in memory.
217       smartcard - the key is stored in a smartcard.
218       token - the key is stored in a hardware token.
219       MobileDevice - the key is stored in a mobile device.
220       MobileAuthCard - the key is stored in a mobile authentication card.
221     </xs:documentation>
222   </xs:annotation>
223 </xs:element>
224 <xs:element name="Password" type="PasswordType">
225   <xs:annotation>
226     <xs:documentation>
227       This element indicates that a password (or passphrase) has been used to
228       authenticate the Principal to a remote system.
229     </xs:documentation>
230   </xs:annotation>
231 </xs:element>
232 <xs:element name="ActivationPin" type="ActivationPinType">
233   <xs:annotation>
234     <xs:documentation>
235       This element indicates that a Pin (Personal Identification Number) has been used to auth
236 nticate the Principal to some local system in order to activate a key.
237     </xs:documentation>
238   </xs:annotation>
239 </xs:element>
240 <xs:element name="Token" type="TokenType">
241   <xs:annotation>
242     <xs:documentation>
243       This element indicates that a hardware or software token is used
244       as a method of identifying the Principal.
245     </xs:documentation>
246   </xs:annotation>
247 </xs:element>
248 <xs:element name="TimeSyncToken" type="TimeSyncTokenType">
249   <xs:annotation>
250     <xs:documentation>
251       This element indicates that a time synchronization
252       token is used to identify the Principal. hardware - the time synchronizati
253       on token has been implemented in hardware. software - the time synchronizati
254       on token has been implemented in software. SeedLength - the length, in bits, of the
255       random seed used in the time synchronization token.
256     </xs:documentation>
257   </xs:annotation>
258 </xs:element>
259 <xs:element name="Smartcard">
260   <xs:annotation>
261     <xs:documentation>
262       This element indicates that a smartcard is used to identify the Principal.
263     </xs:documentation>
264   </xs:annotation>
265 <xs:complexType>
266   <xs:sequence>
267     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
268   </xs:sequence>
269 </xs:complexType>

```

```

270     </xs:element>
271     <xs:element name="Length" type="LengthType">
272         <xs:annotation>
273             <xs:documentation>
274                 This element indicates the minimum and/or maximum ASCII length of the password which is
275                 enforced (by the UA or the IdP). In other words, this is the minimum and/or maximum number of ASCII
276                 I characters required to represent a valid password.
277                 min - the minimum number of ASCII characters required in a valid password, as enforced
278                 by the UA or the IdP.
279                 max - the maximum number of ASCII characters required in a valid password, as enforced
280                 by the UA or the IdP.
281             </xs:documentation>
282         </xs:annotation>
283     </xs:element>
284     <xs:element name="ActivationLimit" type="ActivationLimitType">
285         <xs:annotation>
286             <xs:documentation>
287                 This element indicates the length of time for which an PIN-based authentication is vali
288                 d.
289             </xs:documentation>
290         </xs:annotation>
291     </xs:element>
292     <xs:element name="Generation">
293         <xs:annotation>
294             <xs:documentation>
295                 Indicates whether the password was chosen by the Principal or auto-supplied by the
296                 Authentication Authority.
297                 principalchosen - the Principal is allowed to choose the value of the password. This is
298                 true even if
299                 the initial password is chosen at random by the UA or the IdP and the Principal is then
300                 free to change
301                 the password.
302                 automatic - the password is chosen by the UA or the IdP to be cryptographically strong
303                 in some sense,
304                 or to satisfy certain password rules, and that the Principal is not free to change it
305                 or to choose a new password.
306             </xs:documentation>
307         </xs:annotation>
308         <xs:complexType>
309             <xs:attribute name="mechanism" use="required">
310                 <xs:simpleType>
311                     <xs:restriction base="xs:NMTOKEN">
312                         <xs:enumeration value="principalchosen"/>
313                         <xs:enumeration value="automatic"/>
314                     </xs:restriction>
315                 </xs:simpleType>
316             </xs:attribute>
317         </xs:complexType>
318     </xs:element>
319     <xs:element name="AuthenticationMethod" type="AuthenticationMethodType">
320         <xs:annotation>
321             <xs:documentation>
322                 Refers to those characteristics that define the mechanisms by which the Principal
323                 authenticates to the Authentication Authority.
324             </xs:documentation>
325         </xs:annotation>
326     </xs:element>
327     <xs:element name="PrincipalAuthenticationMechanism" type="PrincipalAuthenticationMechanismType">
328         <xs:annotation>
329             <xs:documentation>
330                 The method that a Principal employs to perform authentication to local system com
331                 ponents.
332             </xs:documentation>
333         </xs:annotation>
334     </xs:element>
335     <xs:element name="Authenticator" type="AuthenticatorType">

```

```

337     <xs:annotation>
338     <xs:documentation>
339         The method applied to validate a principal's authentication across a network
340     </xs:documentation>
341 </xs:annotation>
342 </xs:element>
343 <xs:element name="PreviousSession">
344     <xs:annotation>
345     <xs:documentation>
346         Indicates that the Principal has been strongly authenticated in a previous session,
347 during which the IdP has set a cookie in the UA. During the present session the Principal has only
348 been authenticated by the UA returning the cookie to the IdP.
349     </xs:documentation>
350 </xs:annotation>
351 <xs:complexType>
352     <xs:sequence>
353         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
354     </xs:sequence>
355 </xs:complexType>
356 </xs:element>
357
358 <xs:element name="ResumeSession">
359     <xs:annotation>
360     <xs:documentation>
361         Rather like PreviousSession but using stronger security. A secret that was established
362 in a previous session with the Authentication Authority has been cached by the local system and is
363 now re-used (e.g. a Master Secret is used to derive new session keys in TLS, SSL, WTLS).
364     </xs:documentation>
365 </xs:annotation>
366 <xs:complexType>
367     <xs:sequence>
368         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
369     </xs:sequence>
370 </xs:complexType>
371 </xs:element>
372
373 <xs:element name="ZeroKnowledge">
374     <xs:annotation>
375     <xs:documentation>
376         This element indicates that the Principal has been authenticated by a zero knowledge
377 technique as specified in ISO/IEC 9798-5.
378     </xs:documentation>
379 </xs:annotation>
380 <xs:complexType>
381     <xs:sequence>
382         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
383     </xs:sequence>
384 </xs:complexType>
385 </xs:element>
386 <xs:element name="SharedSecretChallengeResponse">
387     <xs:annotation>
388     <xs:documentation>
389         This element indicates that the Principal has been authenticated by a challenge-response
390 protocol utilizing shared secret keys and symmetric cryptography.
391     </xs:documentation>
392 </xs:annotation>
393 <xs:complexType>
394     <xs:sequence>
395         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
396     </xs:sequence>
397 </xs:complexType>
398 </xs:element>
399 <xs:element name="DigSig">
400     <xs:annotation>
401     <xs:documentation>
402         This element indicates that the Principal has been authenticated by a mechanism which
403 involves the Principal computing a digital signature over at least challenge data provided by the
  
```

```

404 IdP.
405     </xs:documentation>
406     </xs:annotation>
407     <xs:complexType>
408         <xs:sequence>
409             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
410         </xs:sequence>
411     </xs:complexType>
412 </xs:element>
413
414 <xs:element name="IPAddress">
415     <xs:annotation>
416         <xs:documentation>
417             This element indicates that the Principal has been authenticated through connection
418 from a particular IP address.
419         </xs:documentation>
420     </xs:annotation>
421     <xs:complexType>
422         <xs:sequence>
423             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
424         </xs:sequence>
425     </xs:complexType>
426 </xs:element>
427
428 <xs:element name="AsymmetricDecryption">
429     <xs:annotation>
430         <xs:documentation>
431             The local system has a private key but it is used in decryption mode, rather than
432 signature mode. For example, the Authentication Authority generates a secret and encrypts it using
433 the local system's public key: the local system then proves it has decrypted the secret.
434         </xs:documentation>
435     </xs:annotation>
436     <xs:complexType>
437         <xs:sequence>
438             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
439         </xs:sequence>
440     </xs:complexType>
441 </xs:element>
442
443 <xs:element name="AsymmetricKeyAgreement">
444     <xs:annotation>
445         <xs:documentation>
446             The local system has a private key and uses it for shared secret key agreement with t
447 he Authentication Authority (e.g. via Diffie Helman).
448         </xs:documentation>
449     </xs:annotation>
450     <xs:complexType>
451         <xs:sequence>
452             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
453         </xs:sequence>
454     </xs:complexType>
455 </xs:element>
456
457 <xs:element name="SharedSecretDynamicPlaintext">
458     <xs:annotation>
459         <xs:documentation>
460             The local system and Authentication Authority share a secret key. The local system
461 uses this to encrypt a randomised string to pass to the Authentication Authority.
462         </xs:documentation>
463     </xs:annotation>
464     <xs:complexType>
465         <xs:sequence>
466             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
467         </xs:sequence>
468     </xs:complexType>
469 </xs:element>
470

```

```

471     <xs:element name="AuthenticatorTransportProtocol" type="AuthenticatorTransportProtocolType">
472         <xs:annotation>
473             <xs:documentation>
474                 The protocol across which Authenticator information is transferred to an Authentication_
475 Authority verifier.
476             </xs:documentation>
477         </xs:annotation>
478     </xs:element>
479     <xs:element name="HTTP">
480         <xs:annotation>
481             <xs:documentation>
482                 This element indicates that the Authenticator has been transmitted using bare HTTP_
483 utilizing no additional security protocols.
484             </xs:documentation>
485         </xs:annotation>
486         <xs:complexType>
487             <xs:sequence>
488                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
489             </xs:sequence>
490         </xs:complexType>
491     </xs:element>
492     <xs:element name="IPSec">
493         <xs:annotation>
494             <xs:documentation>
495                 This element indicates that the Authenticator has been transmitted using a transport_
496 mechanism protected by an IPSEC session.
497             </xs:documentation>
498         </xs:annotation>
499         <xs:complexType>
500             <xs:sequence>
501                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
502             </xs:sequence>
503         </xs:complexType>
504     </xs:element>
505     <xs:element name="WTLS">
506         <xs:annotation>
507             <xs:documentation>
508                 This element indicates that the Authenticator has been transmitted using a transport_
509 mechanism protected by a WTLS session.
510             </xs:documentation>
511         </xs:annotation>
512         <xs:complexType>
513             <xs:sequence>
514                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
515             </xs:sequence>
516         </xs:complexType>
517     </xs:element>
518     <xs:element name="MobileNetworkNoEncryption">
519         <xs:annotation>
520             <xs:documentation>
521                 This element indicates that the Authenticator has been transmitted solely across a_
522 mobile network using no additional security mechanism.
523             </xs:documentation>
524         </xs:annotation>
525         <xs:complexType>
526             <xs:sequence>
527                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
528             </xs:sequence>
529         </xs:complexType>
530     </xs:element>
531     <xs:element name="MobileNetworkRadioEncryption">
532         <xs:complexType>
533             <xs:sequence>
534                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
535             </xs:sequence>
536         </xs:complexType>
537     </xs:element>

```

```

538 <xs:element name="MobileNetworkEndToEndEncryption">
539   <xs:complexType>
540     <xs:sequence>
541       <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
542     </xs:sequence>
543   </xs:complexType>
544 </xs:element>
545
546   <xs:element name="SSL">
547     <xs:annotation>
548       <xs:documentation>
549         This element indicates that the Authenticator has been transmitted using a transport_
550 mechanism protected by an SSL or TLS session.
551       </xs:documentation>
552     </xs:annotation>
553     <xs:complexType>
554       <xs:sequence>
555         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
556       </xs:sequence>
557     </xs:complexType>
558   </xs:element>
559   <xs:element name="OperationalProtection" type="OperationalProtectionType">
560     <xs:annotation>
561       <xs:documentation>
562         Refers to those characteristics that describe procedural security controls employed by_
563 the Authentication Authority.
564       </xs:documentation>
565     </xs:annotation>
566   </xs:element>
567   <xs:element name="SecurityAudit" type="SecurityAuditType" />
568   <xs:element name="SwitchAudit">
569     <xs:complexType>
570       <xs:sequence>
571         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
572       </xs:sequence>
573     </xs:complexType>
574   </xs:element>
575   <xs:element name="DeactivationCallCenter">
576     <xs:complexType>
577       <xs:sequence>
578         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
579       </xs:sequence>
580     </xs:complexType>
581   </xs:element>
582   <xs:element name="GoverningAgreements" type="GoverningAgreementsType">
583     <xs:annotation>
584       <xs:documentation>
585         Provides a mechanism for linking to external (likely human readable) documents in which_
586 additional business agreements, (e.g. liability constraints, obligations, etc) can be placed.
587       </xs:documentation>
588     </xs:annotation>
589   </xs:element>
590   <xs:element name="GoverningAgreementRef" type="GoverningAgreementRefType" />
591   <xs:element name="AuthenticatingAuthority" type="AuthenticatingAuthorityType">
592     <xs:annotation>
593       <xs:documentation>
594         The Authority that originally authenticated the Principal.
595       </xs:documentation>
596     </xs:annotation>
597   </xs:element>
598 <xs:complexType name="IdentificationType">
599   <xs:sequence>
600     <xs:element ref="PhysicalVerification" minOccurs="0" />
601     <xs:element ref="WrittenConsent" minOccurs="0" />
602     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
603   </xs:sequence>
604   <xs:attribute name="nym">

```

```

605         <xs:annotation>
606             <xs:documentation>
607                 This attribute indicates whether or not the Identification mechanisms allow the
608                 actions of the Principal to be linked to an actual end user.
609             </xs:documentation>
610         </xs:annotation>
611         <xs:simpleType>
612             <xs:restriction base="xs:NMTOKEN">
613                 <xs:enumeration value="anonymity"/>
614                 <xs:enumeration value="verinymity"/>
615                 <xs:enumeration value="pseudonymity"/>
616             </xs:restriction>
617         </xs:simpleType>
618     </xs:attribute>
619 </xs:complexType>
620 <xs:complexType name="GoverningAgreementsType">
621     <xs:sequence>
622         <xs:element ref="GoverningAgreementRef" maxOccurs="unbounded"/>
623     </xs:sequence>
624 </xs:complexType>
625 <xs:complexType name="GoverningAgreementRefType">
626     <xs:attribute name="governingAgreementRef" type="xs:anyURI" use="required"/>
627 </xs:complexType>
628 <xs:complexType name="AuthenticatingAuthorityType">
629     <xs:sequence>
630         <xs:element ref="GoverningAgreements"/>
631     </xs:sequence>
632     <xs:attribute name="ID" type="xs:anyURI" use="required"/>
633 </xs:complexType>
634 <xs:complexType name="AuthenticatorTransportProtocolType">
635     <xs:choice>
636         <xs:element ref="HTTP"/>
637         <xs:element ref="SSL"/>
638         <xs:element ref="MobileNetworkNoEncryption"/>
639         <xs:element ref="MobileNetworkRadioEncryption"/>
640         <xs:element ref="MobileNetworkEndToEndEncryption"/>
641         <xs:element ref="WTLS"/>
642         <xs:element ref="IPSec"/>
643         <xs:element ref="Extension" maxOccurs="unbounded"/>
644     </xs:choice>
645 </xs:complexType>
646 <xs:complexType name="PrincipalAuthenticationMechanismType">
647     <xs:choice>
648         <xs:element ref="Password"/>
649         <xs:element ref="Token"/>
650         <xs:element ref="Smartcard"/>
651         <xs:element ref="ActivationPin"/>
652         <xs:element ref="Extension" maxOccurs="unbounded"/>
653     </xs:choice>
654 </xs:complexType>
655 <xs:complexType name="AuthenticationMethodType">
656     <xs:sequence>
657         <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
658         <xs:element ref="Authenticator" minOccurs="0"/>
659         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
660         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
661     </xs:sequence>
662 </xs:complexType>
663 <xs:complexType name="AuthenticationContextStatementType">
664     <xs:sequence>
665         <xs:element ref="Identification" minOccurs="0"/>
666         <xs:element ref="TechnicalProtection" minOccurs="0"/>
667         <xs:element ref="OperationalProtection" minOccurs="0"/>
668         <xs:element ref="AuthenticationMethod" minOccurs="0"/>
669         <xs:element ref="GoverningAgreements" minOccurs="0"/>
670         <xs:element ref="AuthenticatingAuthority" minOccurs="0"/>
671         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>

```

```

672     </xs:sequence>
673     <xs:attribute name="ID" type="xs:ID"/>
674 </xs:complexType>
675 <xs:complexType name="TechnicalProtectionType">
676     <xs:choice>
677         <xs:element ref="PrivateKeyProtection" minOccurs="0"/>
678         <xs:element ref="SecretKeyProtection" minOccurs="0"/>
679         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
680     </xs:choice>
681 </xs:complexType>
682 <xs:complexType name="OperationalProtectionType">
683     <xs:sequence>
684         <xs:element ref="SecurityAudit" minOccurs="0"/>
685         <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
686         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
687     </xs:sequence>
688 </xs:complexType>
689 <xs:complexType name="AuthenticatorType">
690     <xs:choice>
691         <xs:element ref="PreviousSession"/>
692         <xs:element ref="ResumeSession"/>
693         <xs:element ref="DigSig"/>
694         <xs:element ref="Password"/>
695         <xs:element ref="ZeroKnowledge"/>
696         <xs:element ref="SharedSecretChallengeResponse"/>
697         <xs:element ref="SharedSecretDynamicPlaintext"/>
698         <xs:element ref="IPAddress"/>
699         <xs:element ref="AsymmetricDecryption"/>
700         <xs:element ref="AsymmetricKeyAgreement"/>
701         <xs:element ref="Extension" maxOccurs="unbounded"/>
702     </xs:choice>
703 </xs:complexType>
704 <xs:complexType name="KeyActivationType">
705     <xs:choice>
706         <xs:element ref="ActivationPin"/>
707         <xs:element ref="Extension" maxOccurs="unbounded"/>
708     </xs:choice>
709 </xs:complexType>
710 <xs:complexType name="KeySharingType">
711     <xs:attribute name="sharing" type="xs:boolean" use="required"/>
712 </xs:complexType>
713 <xs:complexType name="PrivateKeyProtectionType">
714     <xs:sequence>
715         <xs:element ref="KeyActivation" minOccurs="0"/>
716         <xs:element ref="KeyStorage" minOccurs="0"/>
717         <xs:element ref="KeySharing" minOccurs="0"/>
718         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
719     </xs:sequence>
720 </xs:complexType>
721
722 <xs:complexType name="PasswordType">
723     <xs:sequence>
724         <xs:element ref="Length" minOccurs="0"/>
725         <xs:element ref="Alphabet" minOccurs="0"/>
726         <xs:element ref="Generation" minOccurs="0"/>
727         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
728     </xs:sequence>
729 </xs:complexType>
730
731 <xs:complexType name="ActivationPinType">
732     <xs:sequence>
733         <xs:element ref="Length" minOccurs="0"/>
734         <xs:element ref="Alphabet" minOccurs="0"/>
735         <xs:element ref="Generation" minOccurs="0"/>
736         <xs:element ref="ActivationLimit" minOccurs="0"/>
737         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
738     </xs:sequence>
    
```



```

739     </xs:complexType>
740
741     <xs:element name="Alphabet" type="AlphabetType"/>
742
743     <xs:complexType name="AlphabetType">
744         <xs:attribute name="requiredChars" type="xs:string" use="required"/>
745         <xs:attribute name="excludedChars" type="xs:string" use="optional"/>
746         <xs:attribute name="case" type="xs:string" use="optional"/>
747     </xs:complexType>
748
749     <xs:complexType name="TokenType">
750         <xs:sequence>
751             <xs:element ref="TimeSyncToken"/>
752             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
753         </xs:sequence>
754     </xs:complexType>
755     <xs:complexType name="TimeSyncToken">
756         <xs:attribute name="DeviceType" use="required">
757             <xs:simpleType>
758                 <xs:restriction base="xs:NMTOKEN">
759                     <xs:enumeration value="hardware"/>
760                     <xs:enumeration value="software"/>
761                 </xs:restriction>
762             </xs:simpleType>
763         </xs:attribute>
764         <xs:attribute name="SeedLength" type="xs:integer" use="required"/>
765         <xs:attribute name="DeviceInHand" use="required">
766             <xs:simpleType>
767                 <xs:restriction base="xs:NMTOKEN">
768                     <xs:enumeration value="true"/>
769                     <xs:enumeration value="false"/>
770                 </xs:restriction>
771             </xs:simpleType>
772         </xs:attribute>
773     </xs:complexType>
774     <xs:complexType name="ActivationLimitType">
775         <xs:choice>
776             <xs:element ref="ActivationLimitDuration"/>
777             <xs:element ref="ActivationLimitUsages"/>
778             <xs:element ref="ActivationLimitSession"/>
779         </xs:choice>
780     </xs:complexType>
781
782     <xs:element name="ActivationLimitDuration" type="ActivationLimitDurationType">
783         <xs:annotation>
784             <xs:documentation>
785                 This element indicates that the Key Activation Limit is defined as a specific duration of
786 time.
787             </xs:documentation>
788         </xs:annotation>
789     </xs:element>
790
791     <xs:element name="ActivationLimitUsages" type="ActivationLimitUsagesType">
792         <xs:annotation>
793             <xs:documentation>
794                 This element indicates that the Key Activation Limit is defined as a number of usages.
795             </xs:documentation>
796         </xs:annotation>
797     </xs:element>
798
799     <xs:element name="ActivationLimitSession" type="ActivationLimitSessionType">
800         <xs:annotation>
801             <xs:documentation>
802                 This element indicates that the Key Activation Limit is the session.
803             </xs:documentation>
804         </xs:annotation>
805     </xs:element>

```

```
806
807 <xs:complexType name="ActivationLimitDurationType">
808   <xs:attribute name="duration" type="xs:duration" use="required"/>
809 </xs:complexType>
810
811 <xs:complexType name="ActivationLimitUsagesType">
812   <xs:attribute name="number" type="xs:integer" use="required"/>
813 </xs:complexType>
814
815 <xs:complexType name="ActivationLimitSessionType"/>
816
817 <xs:complexType name="LengthType">
818   <xs:attribute name="min" type="xs:integer" use="required"/>
819   <xs:attribute name="max" type="xs:integer" use="optional"/>
820 </xs:complexType>
821
822 <xs:complexType name="KeyStorageType">
823   <xs:attribute name="medium" use="required">
824     <xs:simpleType>
825       <xs:restriction base="xs:NMTOKEN">
826         <xs:enumeration value="memory"/>
827         <xs:enumeration value="smartcard"/>
828         <xs:enumeration value="token"/>
829         <xs:enumeration value="MobileDevice"/>
830         <xs:enumeration value="MobileAuthCard"/>
831       </xs:restriction>
832     </xs:simpleType>
833   </xs:attribute>
834 </xs:complexType>
835 <xs:complexType name="SecretKeyProtectionType">
836   <xs:sequence>
837 <xs:element ref="KeyActivation" minOccurs="0"/>
838   <xs:element ref="KeyStorage" minOccurs="0"/>
839   <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
840 </xs:sequence>
841 </xs:complexType>
842 <xs:complexType name="SecurityAuditType">
843   <xs:sequence>
844     <xs:element ref="SwitchAudit" minOccurs="0"/>
845     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
846 </xs:sequence>
847 </xs:complexType>
848 </xs:schema>
849
850
```

851 4.3. Authentication Context Statement Extensibility

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

857 4.4. Authentication Context Statement Processing Rules

858 The processing rules for Authentication Context Statements are listed in [LibProt].

859 **5. Authentication Context Classes**

860 The number of permutations of the different authentication context characteristics ensure that there are a theoretically
861 infinite number of unique authentication contexts. The implication is that in theory any particular relying party would
862 be expected to be able to parse arbitrary authentication context statements and, more importantly, to analyze the
863 statement in order to assess the 'quality' of the associated authentication assertion. Making such an assessment is
864 non-trivial.

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

872 Liberty normalizes this concept through the definition of a number of *Authentication Context Classes*. Each class will
873 define a proper subset of the full set of authentication contexts. Classes have been chosen as representative of the
874 current practices and technologies for authentication technologies. Classes will provide identity and service providers
875 a convenient shorthand when referring to authentication context issues. For instance, an identity provider, may include
876 with the complete authentication context statement it provides to a service provider an assertion that the authentication
877 context also belongs to one of the Liberty defined authentication classes. For some service providers, this assertion
878 will be sufficient detail for it to be able to assign an appropriate level of confidence to the associated authentication
879 assertion. Other service providers might prefer to examine the complete authentication context statement itself.
880 Likewise, the ability to refer to an authentication context class rather than being required to list the complete details
881 of a specific authentication content will simplify how the service provider expresses its desires and/or requirements to
882 an identity provider.

883 **5.1. Advantages of Authentication Context Classes**

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

- 886 • Make it easier for the identity provider and service provider to come to an agreement on what are acceptable
887 authentication contexts by giving them a framework for discussion.
- 888 • Make it easier for service providers to indicate their preferences when requesting a step-up authentication assertion
889 from an identity provider.
- 890 • Simplify for service providers the burden of processing authentication context statements by giving them the option
891 of being satisfied by the associated class.
- 892 • Protect service providers from impact of new authentication technologies.
- 893 • Make it easier for identity providers to publish their authentication capabilities, for example, through WSDL.

894 **5.2. Authentication Context Class Schemas**

895 The initial Liberty authentication context classes are listed in the following sub-sections.

896 The classes are listed in alphabetical order, no ranking is implied by the order of classes.

897 Classes are identified by URIs with the initial stem: <http://www.projectliberty.org/schemas/authctx/classes>

898 The class schemas are defined as extension by restriction of the base Authentication Context schema. Consequently,
899 any XML instances that satisfy the schema constraints of one of the class schemas will also conform to the base
900 Authentication Context schema.

901 **5.2.1. Internet Protocol**

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

903 **5.2.1.1. Associated Liberty URI**

904 <http://www.projectliberty.org/schemas/authctx/classes/InternetProtocol>

905 **5.2.1.2. Class Schema**

```
906
907 <?xml version="1.0" encoding="UTF-8"?>
908 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
909   xmlns:xs="http://www.w3.org/2001/XMLSchema"
910   xmlns="urn:liberty:ac:2003-08"
911   version="1.2-06" finalDefault="extension">
912   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
913   <xs:annotation>
914     <xs:documentation>
915       http://www.projectliberty.org/schemas/authctx/classes/InternetProtocol</xs:documentation>
916     </xs:documentation>
917   </xs:annotation>
918   <xs:complexType name="InternetProtocolAuthenticatorType">
919     <xs:complexContent>
920       <xs:restriction base="AuthenticatorType">
921         <xs:choice>
922           <xs:element ref="IPAddress"/>
923         </xs:choice>
924       </xs:restriction>
925     </xs:complexContent>
926   </xs:complexType>
927 </xs:schema>
928
929
```

930 **5.2.2. InternetProtocolPassword**

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

933 **5.2.2.1. Associated Liberty URI**

934 <http://www.projectliberty.org/schemas/authctx/classes/InternetProtocolPassword>

935 **5.2.2.2. Class Schema**

```
936
937 <?xml version="1.0" encoding="UTF-8"?>
938 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
939   xmlns="urn:liberty:ac:2003-08">
```

```
940 xmlns:xs= "http://www.w3.org/2001/XMLSchema"
941 version="1.2-06" finalDefault="extension">
942 <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
943 <xs:annotation>
944   <xs:documentation>
945     http://www.projectliberty.org/schemas/authctx/classes/InternetProtocolPassword</xs:documentation>
946
947 </xs:annotation>
948
949 <xs:complexType name="InternetProtocolPasswordType">
950   <xs:complexContent>
951     <xs:restriction base="PasswordType">
952       <xs:sequence>
953         <xs:element ref="Length"/>
954         <xs:element ref="Generation" minOccurs="0"/>
955         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
956       </xs:sequence>
957     </xs:restriction>
958   </xs:complexContent>
959 </xs:complexType>
960 <xs:complexType name="InternetProtocolPasswordLengthType">
961   <xs:complexContent>
962     <xs:restriction base="LengthType">
963       <xs:attribute name="min" use="required">
964         <xs:simpleType>
965           <xs:restriction base="xs:integer">
966             <xs:minInclusive value="3"/>
967           </xs:restriction>
968         </xs:simpleType>
969       </xs:attribute>
970       <xs:attribute name="max" type="xs:integer" use="optional"/>
971     </xs:restriction>
972   </xs:complexContent>
973 </xs:complexType>
974 <xs:complexType name="InternetProtocolPasswordAuthenticatorType">
975   <xs:complexContent>
976     <xs:restriction base="AuthenticatorType">
977       <xs:sequence>
978         <xs:element ref="IPAddress"/>
979         <xs:element ref="Password"/>
980         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
981       </xs:sequence>
982     </xs:restriction>
983   </xs:complexContent>
984 </xs:complexType>
985 </xs:schema>
986
987
```

988 5.2.3. MobileOneFactorUnregistered

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

992 5.2.3.1. Associated Liberty URI

993 <http://www.projectliberty.org/schemas/authctx/classes/MobileOneFactorUnregistered>

994 5.2.3.2. Class Schema

```
995
996 <?xml version="1.0" encoding="UTF-8"?>
997 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
998   xmlns="urn:liberty:ac:2003-08"
```

```

999     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1000     finalDefault="extension" version="1.2-08">
1001 <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1002 <xs:annotation>
1003 <xs:documentation>http://www.projectliberty.org/schemas/authctx/classes/MobileOneFactorUnregistered</xs:documentation>
1004 </xs:annotation>
1005 <xs:complexType name="MobileOneFactorUnregisteredAuthenticatorType">
1006 <xs:complexContent>
1007 <xs:restriction base="AuthenticatorType">
1008 <xs:choice>
1009     <xs:element ref="DigSig"/>
1010     <xs:element ref="ZeroKnowledge"/>
1011     <xs:element ref="SharedSecretChallengeResponse"/>
1012     <xs:element ref="AsymmetricDecryption"/>
1013     <xs:element ref="AsymmetricKeyAgreement"/>
1014     <xs:element ref="SharedSecretDynamicPlaintext"/>
1015 </xs:choice>
1016 </xs:restriction>
1017 </xs:complexContent>
1018 </xs:complexType>
1019 <xs:complexType name="MobileOneFactorUnregisteredAuthenticatorTransportProtocolType">
1020 <xs:complexContent>
1021 <xs:restriction base="AuthenticatorTransportProtocolType">
1022 <xs:choice>
1023     <xs:element ref="MobileNetworkNoEncryption"/>
1024     <xs:element ref="MobileNetworkRadioEncryption"/>
1025     <xs:element ref="MobileNetworkEndToEndEncryption"/>
1026     <xs:element ref="WTLS"/>
1027 </xs:choice>
1028 </xs:restriction>
1029 </xs:complexContent>
1030 </xs:complexType>
1031 <xs:complexType name="MobileOneFactorUnregisteredOperationalProtectionType">
1032 <xs:complexContent>
1033 <xs:restriction base="OperationalProtectionType">
1034 <xs:sequence>
1035     <xs:element ref="SecurityAudit"/>
1036     <xs:element ref="DeactivationCallCenter"/>
1037     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1038 </xs:sequence>
1039 </xs:restriction>
1040 </xs:complexContent>
1041 </xs:complexType>
1042 <xs:complexType name="MobileOneFactorUnregisteredTechnicalProtectionType">
1043 <xs:complexContent>
1044 <xs:restriction base="TechnicalProtectionType">
1045 <xs:choice>
1046     <xs:element ref="PrivateKeyProtection"/>
1047     <xs:element ref="SecretKeyProtection"/>
1048 </xs:choice>
1049 </xs:restriction>
1050 </xs:complexContent>
1051 </xs:complexType>
1052 <xs:complexType name="MobileOneFactorUnregisteredPrivateKeyProtectionType">
1053 <xs:complexContent>
1054 <xs:restriction base="PrivateKeyProtectionType">
1055 <xs:sequence>
1056     <xs:element ref="KeyStorage"/>
1057     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1058 </xs:sequence>
1059 </xs:restriction>
1060 </xs:complexContent>
1061 </xs:complexType>
1062 <xs:complexType name="MobileOneFactorUnregisteredSecretKeyProtectionType">
1063 <xs:complexContent>
1064 <xs:restriction base="SecretKeyProtectionType">
1065

```

```

1066 <xs:sequence>
1067 <xs:element ref="KeyStorage" />
1068 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1069 </xs:sequence>
1070 </xs:restriction>
1071 </xs:complexContent>
1072 </xs:complexType>
1073 <xs:complexType name="MobileOneFactorUnregisteredKeyStorageType">
1074 <xs:complexContent>
1075 <xs:restriction base="KeyStorageType">
1076 <xs:attribute name="medium" use="required">
1077 <xs:simpleType>
1078 <xs:restriction base="xs:NMTOKEN">
1079 <xs:enumeration value="MobileDevice" />
1080 <xs:enumeration value="MobileAuthCard" />
1081 <xs:enumeration value="smartcard" />
1082 </xs:restriction>
1083 </xs:simpleType>
1084 </xs:attribute>
1085 </xs:restriction>
1086 </xs:complexContent>
1087 </xs:complexType>
1088 <xs:complexType name="MobileOneFactorUnregisteredSecurityAuditType">
1089 <xs:complexContent>
1090 <xs:restriction base="SecurityAuditType">
1091 <xs:sequence>
1092 <xs:element ref="SwitchAudit" />
1093 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1094 </xs:sequence>
1095 </xs:restriction>
1096 </xs:complexContent>
1097 </xs:complexType>
1098 <xs:complexType name="MobileOneFactorUnregisteredIdentificationType">
1099 <xs:complexContent>
1100 <xs:restriction base="IdentificationType">
1101 <xs:attribute name="nym">
1102 <xs:simpleType>
1103 <xs:restriction base="xs:NMTOKEN">
1104 <xs:enumeration value="anonymity" />
1105 <xs:enumeration value="pseudonymity" />
1106 </xs:restriction>
1107 </xs:simpleType>
1108 </xs:attribute>
1109 </xs:restriction>
1110 </xs:complexContent>
1111 </xs:complexType>
1112 </xs:schema>
1113
1114

```

1115 5.2.4. MobileTwoFactorUnregistered

1116 Reflects no mobile customer registration procedures and a two-factor based authentication, such as secure device and
1117 user PIN. This context class is useful when a service other than the mobile operator wants to link their customer ID
1118 to a mobile supplied two-factor authentication service by capturing mobile phone data at enrollment.

1119 5.2.4.1. Associated Liberty URI

1120 <http://www.projectliberty.org/schemas/authctx/classes/MobileTwoFactorUnregistered>

1121 5.2.4.2. Class Schema

```

1122
1123 <?xml version="1.0" encoding="UTF-8"?>
1124 <xs:schema targetNamespace="urn:liberty:ac:2003-08"

```

```

1125     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1126     xmlns="urn:liberty:ac:2003-08"
1127     version="1.2-08"
1128     finalDefault="extension">
1129     <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1130     <xs:annotation><xs:documentation>http://www.projectliberty.org/schemas/authctx/classes/MobileT
1131 woFactorUnregistered</xs:documentation>
1132 </xs:annotation>
1133
1134     <xs:complexType name="MobileTwoFactorUnregisteredAuthenticatorType">
1135     <xs:complexContent>
1136     <xs:restriction base="AuthenticatorType">
1137         <xs:choice>
1138             <xs:element ref="DigSig"/>
1139             <xs:element ref="ZeroKnowledge"/>
1140             <xs:element ref="SharedSecretChallengeResponse"/>
1141             <xs:element ref="AsymmetricDecryption"/>
1142             <xs:element ref="AsymmetricKeyAgreement"/>
1143             <xs:element ref="SharedSecretDynamicPlaintext"/>
1144             <xs:sequence>
1145                 <xs:element ref="Password" minOccurs="1"/>
1146                 <xs:choice>
1147                     <xs:element ref="SharedSecretDynamicPlaintext"/>
1148                     <xs:element ref="SharedSecretChallengeResponse"/>
1149                 </xs:choice>
1150                 <xs:element ref="Extension" maxOccurs="unbounded"/>
1151             </xs:sequence>
1152         </xs:choice>
1153     </xs:restriction>
1154 </xs:complexContent>
1155 </xs:complexType>
1156     <xs:complexType name="MobileTwoFactorUnregisteredAuthenticatorTransportProtocolType">
1157     <xs:complexContent>
1158     <xs:restriction base="AuthenticatorTransportProtocolType">
1159         <xs:choice>
1160             <xs:element ref="MobileNetworkNoEncryption"/>
1161             <xs:element ref="MobileNetworkRadioEncryption"/>
1162             <xs:element ref="MobileNetworkEndToEndEncryption"/>
1163             <xs:element ref="WTLS"/>
1164         </xs:choice>
1165     </xs:restriction>
1166 </xs:complexContent>
1167 </xs:complexType>
1168     <xs:complexType name="MobileTwoFactorUnregisteredOperationalProtectionType">
1169     <xs:complexContent>
1170     <xs:restriction base="OperationalProtectionType">
1171         <xs:sequence>
1172             <xs:element ref="SecurityAudit"/>
1173             <xs:element ref="DeactivationCallCenter"/>
1174             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1175         </xs:sequence>
1176     </xs:restriction>
1177 </xs:complexContent>
1178 </xs:complexType>
1179     <xs:complexType name="MobileTwoFactorUnregisteredTechnicalProtectionType">
1180     <xs:complexContent>
1181     <xs:restriction base="TechnicalProtectionType">
1182         <xs:choice>
1183             <xs:element ref="PrivateKeyProtection"/>
1184             <xs:element ref="SecretKeyProtection"/>
1185         </xs:choice>
1186     </xs:restriction>
1187 </xs:complexContent>
1188 </xs:complexType>
1189
1190     <xs:complexType name="MobileTwoFactorUnregisteredPrivateKeyProtectionType">
1191     <xs:complexContent>

```



```

1192     <xs:restriction base="PrivateKeyProtectionType">
1193         <xs:sequence>
1194             <xs:element ref="KeyActivation" minOccurs="1" maxOccurs="1"/>
1195             <xs:element ref="KeyStorage" minOccurs="0"/>
1196             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1197         </xs:sequence>
1198     </xs:restriction>
1199 </xs:complexContent>
1200 </xs:complexType>
1201
1202 <xs:complexType name="MobileTwoFactorUnregisteredSecretKeyProtectionType">
1203     <xs:complexContent>
1204         <xs:restriction base="SecretKeyProtectionType">
1205             <xs:sequence>
1206                 <xs:element ref="KeyActivation"/>
1207                 <xs:element ref="KeyStorage"/>
1208                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1209             </xs:sequence>
1210         </xs:restriction>
1211     </xs:complexContent>
1212 </xs:complexType>
1213
1214 <xs:complexType name="MobileTwoFactorUnregisteredKeyActivationType">
1215     <xs:complexContent>
1216         <xs:restriction base="KeyActivationType">
1217             <xs:sequence>
1218                 <xs:element ref="ActivationPin"/>
1219                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1220             </xs:sequence>
1221         </xs:restriction>
1222     </xs:complexContent>
1223 </xs:complexType>
1224
1225 <xs:complexType name="MobileTwoFactorUnregisteredKeyType">
1226     <xs:complexContent>
1227         <xs:restriction base="KeyType">
1228             <xs:attribute name="medium" use="required" />
1229             <xs:simpleType>
1230                 <xs:restriction base="xs:NMTOKEN">
1231                     <xs:enumeration value="MobileDevice"/>
1232                     <xs:enumeration value="MobileAuthCard"/>
1233                     <xs:enumeration value="smartcard"/>
1234                 </xs:restriction>
1235             </xs:simpleType>
1236         </xs:attribute>
1237     </xs:restriction>
1238 </xs:complexContent>
1239 </xs:complexType>
1240
1241 <xs:complexType name="MobileTwoFactorUnregisteredSecurityAuditType">
1242     <xs:complexContent>
1243         <xs:restriction base="SecurityAuditType">
1244             <xs:sequence>
1245                 <xs:element ref="SwitchAudit"/>
1246                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1247             </xs:sequence>
1248         </xs:restriction>
1249     </xs:complexContent>
1250 </xs:complexType>
1251
1252 <xs:complexType name="MobileTwoFactorUnregisteredIdentificationType">
1253     <xs:complexContent>
1254         <xs:restriction base="IdentificationType">
1255             <xs:attribute name="nym" />
1256         <xs:simpleType>
1257             <xs:restriction base="xs:NMTOKEN">
1258                 <xs:enumeration value="anonymity"/>

```

```

1259     <xs:enumeration value="pseudonymity"/>
1260 </xs:restriction>
1261 </xs:simpleType>
1262 </xs:attribute>
1263 </xs:restriction>
1264 </xs:complexContent>
1265 </xs:complexType>
1266
1267 </xs:schema>
1268
1269

```

1270 5.2.5. MobileOneFactorContract

1271 Reflects mobile contract customer registration procedures and a single factor authentication. For example, a digital
1272 signing device with tamper resistant memory for key storage, such as the mobile MSISDN, but no required PIN or
1273 biometric for real-time user authentication.

1274 5.2.5.1. Associated Liberty URI

1275 <http://www.projectliberty.org/schemas/authctx/classes/MobileOneFactorContract>

1276 5.2.5.2. Class Schema

```

1277
1278 <?xml version="1.0" encoding="UTF-8"?>
1279 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1280     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1281     xmlns="urn:liberty:ac:2003-08"
1282     version="1.2-08" finalDefault="extension">
1283     <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1284     <xs:annotation>
1285 <xs:documentation>http://www.projectliberty.org/schemas/authctx/classes/MobileOneFactorContract</xs:documentation>
1286 </xs:annotation>
1287
1288     <xs:complexType name="MobileOneFactorContractAuthenticatorType">
1289         <xs:complexContent>
1290             <xs:restriction base="AuthenticatorType">
1291                 <xs:choice maxOccurs="1">
1292                     <xs:element ref="DigSig"/>
1293                     <xs:element ref="ZeroKnowledge"/>
1294                     <xs:element ref="SharedSecretChallengeResponse"/>
1295                     <xs:element ref="AsymmetricDecryption"/>
1296                     <xs:element ref="AsymmetricKeyAgreement"/>
1297                     <xs:element ref="SharedSecretDynamicPlaintext"/>
1298                 </xs:choice>
1299             </xs:restriction>
1300         </xs:complexContent>
1301     </xs:complexType>
1302     <xs:complexType name="MobileOneFactorContractAuthenticatorTransportProtocolType">
1303         <xs:complexContent>
1304             <xs:restriction base="AuthenticatorTransportProtocolType">
1305                 <xs:choice>
1306                     <xs:element ref="MobileNetworkNoEncryption"/>
1307                     <xs:element ref="MobileNetworkRadioEncryption"/>
1308                     <xs:element ref="MobileNetworkEndToEndEncryption"/>
1309                     <xs:element ref="WTLS"/>
1310                 </xs:choice>
1311             </xs:restriction>
1312         </xs:complexContent>
1313     </xs:complexType>
1314     <xs:complexType name="MobileOneFactorContractOperationalProtectionType">
1315         <xs:complexContent>
1316             <xs:restriction base="OperationalProtectionType">
1317                 <xs:sequence>

```

```
1318         <xs:element ref="SecurityAudit" />
1319         <xs:element ref="DeactivationCallCenter" />
1320         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1321     </xs:sequence>
1322 </xs:restriction>
1323 </xs:complexContent>
1324 </xs:complexType>
1325 <xs:complexType name="MobileOneFactorContractTechnicalProtectionType">
1326     <xs:complexContent>
1327         <xs:restriction base="TechnicalProtectionType">
1328             <xs:choice>
1329                 <xs:element ref="PrivateKeyProtection" />
1330                 <xs:element ref="SecretKeyProtection" />
1331             </xs:choice>
1332         </xs:restriction>
1333     </xs:complexContent>
1334 </xs:complexType>
1335
1336 <xs:complexType name="MobileOneFactorContractPrivateKeyProtectionType">
1337     <xs:complexContent>
1338         <xs:restriction base="PrivateKeyProtectionType">
1339             <xs:sequence maxOccurs="1">
1340                 <xs:element ref="KeyStorage" />
1341                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1342             </xs:sequence>
1343         </xs:restriction>
1344     </xs:complexContent>
1345 </xs:complexType>
1346
1347 <xs:complexType name="MobileOneFactorContractSecretKeyProtectionType">
1348     <xs:complexContent>
1349         <xs:restriction base="SecretKeyProtectionType">
1350             <xs:sequence>
1351                 <xs:element ref="KeyStorage" />
1352                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1353             </xs:sequence>
1354         </xs:restriction>
1355     </xs:complexContent>
1356 </xs:complexType>
1357
1358 <xs:complexType name="MobileOneFactorContractKeyStorageType">
1359     <xs:complexContent>
1360         <xs:restriction base="KeyStorageType">
1361             <xs:attribute name="medium" use="required">
1362                 <xs:simpleType>
1363                     <xs:restriction base="xs:NMTOKEN">
1364                         <xs:enumeration value="MobileDevice" />
1365                         <xs:enumeration value="MobileAuthCard" />
1366                         <xs:enumeration value="smartcard" />
1367                     </xs:restriction>
1368                 </xs:simpleType>
1369             </xs:attribute>
1370         </xs:restriction>
1371     </xs:complexContent>
1372 </xs:complexType>
1373
1374 <xs:complexType name="MobileOneFactorContractSecurityAuditType">
1375     <xs:complexContent>
1376         <xs:restriction base="SecurityAuditType">
1377             <xs:sequence>
1378                 <xs:element ref="SwitchAudit" />
1379                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1380             </xs:sequence>
1381         </xs:restriction>
1382     </xs:complexContent>
1383 </xs:complexType>
1384
```

```

1385 <xs:complexType name="MobileOneFactorContractIdentificationType">
1386 <xs:complexContent>
1387 <xs:restriction base="IdentificationType">
1388 <xs:sequence>
1389 <xs:element ref="PhysicalVerification"/>
1390 <xs:element ref="WrittenConsent"/>
1391 <xs:element ref="GoverningAgreements"/>
1392 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1393 </xs:sequence>
1394 <xs:attribute name="nym">
1395 <xs:simpleType>
1396 <xs:restriction base="xs:NMTOKEN">
1397 <xs:enumeration value="anonymity"/>
1398 <xs:enumeration value="verinymity"/>
1399 <xs:enumeration value="pseudonymity"/>
1400 </xs:restriction>
1401 </xs:simpleType>
1402 </xs:attribute>
1403 </xs:restriction>
1404 </xs:complexContent>
1405 </xs:complexType>
1406
1407 </xs:schema>
1408
1409
  
```

1410 5.2.6. MobileTwoFactorContract

1411 Reflects mobile contract customer registration procedures and a two-factor based authentication. For example, a
 1412 digital signing device with tamper resistant memory for key storage, such as a GSM SIM, that requires explicit proof
 1413 of user identity and intent, such as a PIN or biometric.

1414 5.2.6.1. Associated Liberty URI

1415 <http://www.projectliberty.org/schemas/authctx/classes/MobileTwoFactorContract>

1416 5.2.6.2. Class Schema

```

1417
1418 <?xml version="1.0" encoding="UTF-8"?>
1419 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1420 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1421 xmlns="urn:liberty:ac:2003-08"
1422 version="1.2-08"
1423 finalDefault="extension">
1424 <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1425 <xs:annotation><xs:documentation>http://www.projectliberty.org/schemas/authctx/classes/MobileT
1426 woFactorContract</xs:documentation>
1427 </xs:annotation>
1428
1429 <xs:complexType name="MobileTwoFactorContractAuthenticatorType">
1430 <xs:complexContent>
1431 <xs:restriction base="AuthenticatorType">
1432 <xs:choice>
1433 <xs:element ref="DigSig"/>
1434 <xs:element ref="ZeroKnowledge"/>
1435 <xs:element ref="SharedSecretChallengeResponse"/>
1436 <xs:element ref="AsymmetricDecryption"/>
1437 <xs:element ref="AsymmetricKeyAgreement"/>
1438 <xs:element ref="SharedSecretDynamicPlaintext"/>
1439 <xs:sequence>
1440 <xs:element ref="Password" minOccurs="1"/>
1441 <xs:choice>
1442 <xs:element ref="SharedSecretDynamicPlaintext"/>
1443 <xs:element ref="SharedSecretChallengeResponse"/>
  
```

```

1444         </xs:choice>
1445         <xs:element ref="Extension" maxOccurs="unbounded" />
1446     </xs:sequence>
1447 </xs:choice>
1448 </xs:restriction>
1449 </xs:complexContent>
1450 </xs:complexType>
1451 <xs:complexType name="MobileTwoFactorContractAuthenticatorTransportProtocolType">
1452     <xs:complexContent>
1453         <xs:restriction base="AuthenticatorTransportProtocolType">
1454             <xs:choice>
1455                 <xs:element ref="MobileNetworkNoEncryption" />
1456                 <xs:element ref="MobileNetworkRadioEncryption" />
1457                 <xs:element ref="MobileNetworkEndToEndEncryption" />
1458                 <xs:element ref="WTLS" />
1459             </xs:choice>
1460         </xs:restriction>
1461     </xs:complexContent>
1462 </xs:complexType>
1463 <xs:complexType name="MobileTwoFactorContractOperationalProtectionType">
1464     <xs:complexContent>
1465         <xs:restriction base="OperationalProtectionType">
1466             <xs:sequence>
1467                 <xs:element ref="SecurityAudit" />
1468                 <xs:element ref="DeactivationCallCenter" />
1469                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1470             </xs:sequence>
1471         </xs:restriction>
1472     </xs:complexContent>
1473 </xs:complexType>
1474 <xs:complexType name="MobileTwoFactorContractTechnicalProtectionType">
1475     <xs:complexContent>
1476         <xs:restriction base="TechnicalProtectionType">
1477             <xs:choice>
1478                 <xs:element ref="PrivateKeyProtection" />
1479                 <xs:element ref="SecretKeyProtection" />
1480             </xs:choice>
1481         </xs:restriction>
1482     </xs:complexContent>
1483 </xs:complexType>
1484
1485 <xs:complexType name="MobileTwoFactorContractPrivateKeyProtectionType">
1486     <xs:complexContent>
1487         <xs:restriction base="PrivateKeyProtectionType">
1488             <xs:sequence>
1489                 <xs:element ref="KeyActivation" minOccurs="1" maxOccurs="1" />
1490                 <xs:element ref="KeyStorage" minOccurs="0" />
1491                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1492             </xs:sequence>
1493         </xs:restriction>
1494     </xs:complexContent>
1495 </xs:complexType>
1496
1497 <xs:complexType name="MobileTwoFactorContractSecretKeyProtectionType">
1498     <xs:complexContent>
1499         <xs:restriction base="SecretKeyProtectionType">
1500             <xs:sequence>
1501                 <xs:element ref="KeyActivation" />
1502                 <xs:element ref="KeyStorage" />
1503                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1504             </xs:sequence>
1505         </xs:restriction>
1506     </xs:complexContent>
1507 </xs:complexType>
1508
1509 <xs:complexType name="MobileTwoFactorContractKeyActivationType">
1510     <xs:complexContent>

```

```

1511     <xs:restriction base="KeyActivationType">
1512     <xs:sequence>
1513     <xs:element ref="ActivationPin"/>
1514     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1515     </xs:sequence>
1516     </xs:restriction>
1517 </xs:complexContent>
1518 </xs:complexType>
1519
1520 <xs:complexType name="MobileTwoFactorContractKeyStorageType">
1521 <xs:complexContent>
1522 <xs:restriction base="KeyStorageType">
1523 <xs:attribute name="medium" use="required">
1524 <xs:simpleType>
1525 <xs:restriction base="xs:NMTOKEN">
1526 <xs:enumeration value="MobileDevice"/>
1527 <xs:enumeration value="MobileAuthCard"/>
1528 <xs:enumeration value="smartcard"/>
1529 </xs:restriction>
1530 </xs:simpleType>
1531 </xs:attribute>
1532 </xs:restriction>
1533 </xs:complexContent>
1534 </xs:complexType>
1535
1536 <xs:complexType name="MobileTwoFactorContractSecurityAuditType">
1537 <xs:complexContent>
1538 <xs:restriction base="SecurityAuditType">
1539 <xs:sequence>
1540 <xs:element ref="SwitchAudit"/>
1541 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1542 </xs:sequence>
1543 </xs:restriction>
1544 </xs:complexContent>
1545 </xs:complexType>
1546
1547 <xs:complexType name="MobileTwoFactorContractIdentificationType">
1548 <xs:complexContent>
1549 <xs:restriction base="IdentificationType">
1550 <xs:sequence>
1551 <xs:element ref="PhysicalVerification"/>
1552 <xs:element ref="WrittenConsent"/>
1553 <xs:element ref="GoverningAgreements"/>
1554 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1555 </xs:sequence>
1556 <xs:attribute name="nym">
1557 <xs:simpleType>
1558 <xs:restriction base="xs:NMTOKEN">
1559 <xs:enumeration value="anonymity"/>
1560 <xs:enumeration value="veronymity"/>
1561 <xs:enumeration value="pseudonymity"/>
1562 </xs:restriction>
1563 </xs:simpleType>
1564 </xs:attribute>
1565 </xs:restriction>
1566 </xs:complexContent>
1567 </xs:complexType>
1568 </xs:schema>
1569
1570

```

1571 5.2.7. Password

1572 The Password class is identified when a Principal authenticates to an identity provider through the presentation of a
 1573 password over an unprotected HTTP session.

1574 5.2.7.1. Associated Liberty URI

1575 <http://www.projectliberty.org/schemas/authctx/classes/Password>

1576 5.2.7.2. Class Schema

```
1577
1578 <?xml version="1.0" encoding="UTF-8"?>
1579 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1580   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1581   xmlns="urn:liberty:ac:2003-08"
1582   version="1.2-06"
1583   finalDefault="extension">
1584   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1585   <xs:annotation>
1586     <xs:documentation>
1587       http://www.projectliberty.org/schemas/authctx/classes/Password</xs:documentation>
1588     </xs:annotation>
1589   <xs:complexType name="PasswordAuthenticatorType">
1590     <xs:complexContent>
1591       <xs:restriction base="AuthenticatorType">
1592         <xs:choice>
1593           <xs:element ref="Password"/>
1594         </xs:choice>
1595       </xs:restriction>
1596     </xs:complexContent>
1597   </xs:complexType>
1598
1599   <xs:complexType name="PasswordPasswordType">
1600     <xs:complexContent>
1601       <xs:restriction base="PasswordType">
1602         <xs:sequence>
1603           <xs:element ref="Length" minOccurs="1"/>
1604           <xs:element ref="Generation" minOccurs="0"/>
1605           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1606         </xs:sequence>
1607       </xs:restriction>
1608     </xs:complexContent>
1609   </xs:complexType>
1610
1611   <xs:complexType name="PasswordLengthType">
1612     <xs:complexContent>
1613       <xs:restriction base="LengthType">
1614         <xs:attribute name="min" use="required">
1615           <xs:simpleType>
1616             <xs:restriction base="xs:integer">
1617               <xs:minInclusive value="3"/>
1618             </xs:restriction>
1619           </xs:simpleType>
1620         </xs:attribute>
1621         <xs:attribute name="max" type="xs:integer" use="optional"/>
1622       </xs:restriction>
1623     </xs:complexContent>
1624   </xs:complexType>
1625
1626 </xs:schema>
1627
1628
```

1629 5.2.8. PasswordProtectedTransport

1630 The PasswordProtectedTransport class is identified when a Principal authenticates to an identity provider through the
1631 presentation of a password over a protected session.

1632 5.2.8.1. Associated Liberty URI

1633 <http://www.projectliberty.org/schemas/authctx/classes/PasswordProtectedTransport>

1634 5.2.8.2. Class Schema

```

1635
1636 <?xml version="1.0" encoding="UTF-8"?>
1637 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1638   xmlns="urn:liberty:ac:2003-08"
1639   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1640   version="1.2-06"
1641   finalDefault="extension">
1642   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1643   <xs:annotation>
1644     <xs:documentation>
1645       http://www.projectliberty.org/schemas/authctx/classes/PasswordProtectedTransport</xs:documentatio
1646 n>
1647   </xs:annotation>
1648   <xs:complexType name="PasswordProtectedTransportAuthenticatorType">
1649     <xs:complexContent>
1650       <xs:restriction base="AuthenticatorType">
1651         <xs:choice>
1652           <xs:element ref="Password"/>
1653         </xs:choice>
1654       </xs:restriction>
1655     </xs:complexContent>
1656   </xs:complexType>
1657
1658   <xs:complexType name="PasswordProtectedTransportPasswordType">
1659     <xs:complexContent>
1660       <xs:restriction base="PasswordType">
1661         <xs:sequence>
1662           <xs:element ref="Length"/>
1663           <xs:element ref="Generation" minOccurs="0"/>
1664           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1665         </xs:sequence>
1666       </xs:restriction>
1667     </xs:complexContent>
1668   </xs:complexType>
1669
1670   <xs:complexType name="PasswordProtectedTransportLengthType">
1671     <xs:complexContent>
1672       <xs:restriction base="LengthType">
1673         <xs:attribute name="min" use="required">
1674           <xs:simpleType>
1675             <xs:restriction base="xs:integer">
1676               <xs:minInclusive value="3"/>
1677             </xs:restriction>
1678           </xs:simpleType>
1679         </xs:attribute>
1680         <xs:attribute name="max" type="xs:integer" use="optional"/>
1681       </xs:restriction>
1682     </xs:complexContent>
1683   </xs:complexType>
1684   <xs:complexType name="PasswordProtectedTransportAuthenticatorTransportProtocolType">
1685     <xs:complexContent>
1686       <xs:restriction base="AuthenticatorTransportProtocolType">
1687         <xs:choice>
1688           <xs:element ref="SSL"/>
1689         </xs:choice>
1690       </xs:restriction>
1691     </xs:complexContent>
1692   </xs:complexType>
1693 </xs:schema>
1694
1695

```


1696 **5.2.9. PreviousSession**

1697 The PreviousSession class is identified when a Principal had authenticated to an identity provider at some point in the
1698 past using any authentication context supported by that identity provider. Consequently, a subsequent authentication
1699 event that the identity provider will assert to the service provider may be significantly separated in time from the
1700 Principals current resource access request.

1701 The context for the previously authenticated session is explicitly not included in this context class because the user
1702 has not authenticated during this session, and so the mechanism that the user employed to authenticate in a previous
1703 session should not be used as part of a decision on whether to now allow access to a resource.

1704 **5.2.9.1. Associated Liberty URI**

1705 <http://www.projectliberty.org/schemas/authctx/classes/PreviousSession>

1706 **5.2.9.2. Class Schema**

```
1707
1708 <?xml version="1.0" encoding="UTF-8"?>
1709 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1710   xmlns="urn:liberty:ac:2003-08"
1711   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1712   version="1.2-06"
1713   finalDefault="extension">
1714   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1715   <xs:annotation>
1716     <xs:documentation>
1717       http://www.projectliberty.org/schemas/authctx/classes/PreviousSession</xs:documentation>
1718   </xs:annotation>
1719   <xs:complexType name="PreviousSessionAuthenticatorType">
1720     <xs:complexContent>
1721       <xs:restriction base="AuthenticatorType">
1722         <xs:choice>
1723           <xs:element ref="PreviousSession"/>
1724         </xs:choice>
1725       </xs:restriction>
1726     </xs:complexContent>
1727   </xs:complexType>
1728 </xs:schema>
1729
1730
1731
```

1732 **5.2.10. Smartcard**

1733 The Smartcard class is identified when a Principal authenticates to an identity provider using a smartcard.

1734 **5.2.10.1. Associated Liberty URI**

1735 <http://www.projectliberty.org/schemas/authctx/classes/Smartcard>

1736 **5.2.10.2. Class Schema**

```
1737
1738 <?xml version="1.0" encoding="UTF-8"?>
1739 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1740   xmlns="urn:liberty:ac:2003-08"
1741   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1742   version="1.2-06"
1743   finalDefault="extension">
1744   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1745   <xs:annotation>
1746     <xs:documentation> http://www.projectliberty.org/schemas/authctx/classes/Smartcard
```

```

1747 </xs:documentation>
1748 </xs:annotation>
1749 <xs:complexType name="SmartCardPrincipalAuthenticationMechanismType">
1750 <xs:complexContent>
1751 <xs:restriction base="PrincipalAuthenticationMechanismType">
1752 <xs:choice>
1753 <xs:element ref="Smartcard"/>
1754 </xs:choice>
1755 </xs:restriction>
1756 </xs:complexContent>
1757 </xs:complexType>
1758 </xs:schema>
1759
1760
  
```

1761 5.2.11. SmartcardPKI

1762 The SmartcardPKI class is identified when a Principal authenticates to an identity provider through a two-factor
 1763 authentication mechanism using a smartcard with enclosed private key and a PIN.

1764 5.2.11.1. Associated Liberty URI

1765 <http://www.projectliberty.org/schemas/authctx/classes/SmartcardPKI>

1766 5.2.11.2. Class Schema

```

1767
1768 <?xml version="1.0" encoding="UTF-8"?>
1769 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1770 xmlns="urn:liberty:ac:2003-08"
1771 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1772 version="1.2-06"
1773 finalDefault="extension">
1774 <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1775 <xs:annotation>
1776 <xs:documentation>
1777 http://www.projectliberty.org/schemas/authctx/classes/SmartcardPKI</xs:documentation>
1778 </xs:annotation>
1779
1780 <xs:complexType name="SmartCardPKIPrincipalAuthenticationMechanismType">
1781 <xs:complexContent>
1782 <xs:restriction base="PrincipalAuthenticationMechanismType">
1783 <xs:sequence>
1784 <xs:element ref="ActivationPin"/>
1785 <xs:element ref="Smartcard"/>
1786 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1787 </xs:sequence>
1788 </xs:restriction>
1789 </xs:complexContent>
1790 </xs:complexType>
1791
1792 <xs:complexType name="SmartCardPKIAuthenticatorType">
1793 <xs:complexContent>
1794 <xs:restriction base="AuthenticatorType">
1795 <xs:choice>
1796 <xs:element ref="AsymmetricDecryption"/>
1797 <xs:element ref="AsymmetricKeyAgreement"/>
1798 <xs:element ref="DigSig"/>
1799 </xs:choice>
1800 </xs:restriction>
1801 </xs:complexContent>
1802 </xs:complexType>
1803
1804 <xs:complexType name="SmartCardPKIKeyActivationType">
1805 <xs:complexContent>
  
```

```

1806         <xs:restriction base="KeyActivationType">
1807             <xs:choice>
1808                 <xs:element ref="ActivationPin" />
1809             </xs:choice>
1810         </xs:restriction>
1811     </xs:complexContent>
1812 </xs:complexType>
1813
1814 <xs:complexType name="SmartcardPKIKeyStorageType">
1815     <xs:complexContent>
1816         <xs:restriction base="KeyStorageType">
1817             <xs:attribute name="medium" use="required">
1818                 <xs:simpleType>
1819                     <xs:restriction base="xs:NMTOKEN">
1820                         <xs:enumeration value="smartcard" />
1821                     </xs:restriction>
1822                 </xs:simpleType>
1823             </xs:attribute>
1824         </xs:restriction>
1825     </xs:complexContent>
1826 </xs:complexType>
1827
1828
1829 <xs:complexType name="SmartCardPKIPrivateKeyProtectionType">
1830     <xs:complexContent>
1831         <xs:restriction base="PrivateKeyProtectionType">
1832             <xs:sequence>
1833                 <xs:element ref="KeyActivation" />
1834                 <xs:element ref="KeyStorage" />
1835                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1836             </xs:sequence>
1837         </xs:restriction>
1838     </xs:complexContent>
1839 </xs:complexType>
1840
1841 </xs:schema>
1842
1843
  
```

1844 5.2.12. SoftwarePKI

1845 The Software-PKI class is identified when a Principal uses an X.509 certificate stored in software to authenticate to
 1846 the identity provider.

1847 5.2.12.1. Associated Liberty URI

1848 <http://www.projectliberty.org/schemas/authctx/classes/SoftwarePKI>

1849 5.2.12.2. Class Schema

```

1850
1851 <?xml version="1.0" encoding="UTF-8"?>
1852 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1853     xmlns="urn:liberty:ac:2003-08"
1854     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1855     version="1.2-06"
1856     finalDefault="extension">
1857     <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd" />
1858     <xs:annotation>
1859         <xs:documentation>
1860             http://www.projectliberty.org/schemas/authctx/classes/SoftwarePKI</xs:documentation>
1861         </xs:documentation>
1862     </xs:annotation>
1863     <xs:complexType name="SoftwarePKIPrincipalAuthenticationMechanismType">
1864         <xs:complexContent>
  
```

```

1865         <xs:restriction base="PrincipalAuthenticationMechanismType">
1866             <xs:sequence>
1867                 <xs:element ref="ActivationPin"/>
1868                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1869             </xs:sequence>
1870         </xs:restriction>
1871     </xs:complexContent>
1872 </xs:complexType>
1873
1874 <xs:complexType name="SoftwarePKIAuthenticatorType">
1875     <xs:complexContent>
1876         <xs:restriction base="AuthenticatorType">
1877             <xs:choice>
1878                 <xs:element ref="AsymmetricDecryption"/>
1879                 <xs:element ref="AsymmetricKeyAgreement"/>
1880                 <xs:element ref="DigSig"/>
1881             </xs:choice>
1882         </xs:restriction>
1883     </xs:complexContent>
1884 </xs:complexType>
1885
1886 <xs:complexType name="SoftwarePKIKeyActivationType">
1887     <xs:complexContent>
1888         <xs:restriction base="KeyActivationType">
1889             <xs:choice>
1890                 <xs:element ref="ActivationPin"/>
1891             </xs:choice>
1892         </xs:restriction>
1893     </xs:complexContent>
1894 </xs:complexType>
1895
1896 <xs:complexType name="SoftwarePKI PrivateKeyProtectionType">
1897     <xs:complexContent>
1898         <xs:restriction base="PrivateKeyProtectionType">
1899             <xs:sequence>
1900                 <xs:element ref="KeyActivation"/>
1901                 <xs:element ref="KeyStorage"/>
1902                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1903             </xs:sequence>
1904         </xs:restriction>
1905     </xs:complexContent>
1906 </xs:complexType>
1907
1908 <xs:complexType name="SoftwarePKIKeyStorageType">
1909     <xs:complexContent>
1910         <xs:restriction base="KeyStorageType">
1911             <xs:attribute name="medium" use="required">
1912                 <xs:simpleType>
1913                     <xs:restriction base="xs:NMTOKEN">
1914                         <xs:enumeration value="memory"/>
1915                     </xs:restriction>
1916                 </xs:simpleType>
1917             </xs:attribute>
1918         </xs:restriction>
1919     </xs:complexContent>
1920 </xs:complexType>
1921 </xs:schema>
1922
1923
1924

```

1925 5.2.13. TimeSyncToken

1926 The TimeSyncToken class is identified when a Principal authenticates through a time synchronization token.

1927 5.2.13.1. Associated Liberty URI

1928 <http://www.projectliberty.org/schemas/authctx/classes/TimeSyncToken>

1929 **5.2.13.2. Class Schema**

```
1930
1931 <?xml version="1.0" encoding="UTF-8"?>
1932 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1933     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1934     xmlns="urn:liberty:ac:2003-08"
1935     finalDefault="extension">
1936   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1937   <xs:annotation>
1938     <xs:documentation> http://www.projectliberty.org/schemas/authctx/classes/TimeSyncToken</xs:
1939 documentation>
1940   </xs:annotation>
1941   <xs:complexType name="TimeSyncTokenPrincipalAuthenticationMechanismType">
1942     <xs:complexContent>
1943       <xs:restriction base="PrincipalAuthenticationMechanismType">
1944         <xs:choice>
1945           <xs:element ref="Token"/>
1946         </xs:choice>
1947       </xs:restriction>
1948     </xs:complexContent>
1949   </xs:complexType>
1950   <xs:complexType name="TimeSyncTokenTokenType">
1951     <xs:complexContent>
1952       <xs:restriction base="TokenType">
1953         <xs:sequence>
1954           <xs:element ref="TimeSyncToken"/>
1955           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1956         </xs:sequence>
1957       </xs:restriction>
1958     </xs:complexContent>
1959   </xs:complexType>
1960   <xs:complexType name="TimeSyncTokenTimeSyncTokenType">
1961     <xs:complexContent>
1962       <xs:restriction base="TimeSyncTokenType">
1963         <xs:attribute name="DeviceType" use="required">
1964           <xs:simpleType>
1965             <xs:restriction base="xs:NMTOKEN">
1966               <xs:enumeration value="hardware"/>
1967             </xs:restriction>
1968           </xs:simpleType>
1969         </xs:attribute>
1970         <xs:attribute name="SeedLength" use="required">
1971           <xs:simpleType>
1972             <xs:restriction base="xs:integer">
1973               <xs:enumeration value="64"/>
1974             </xs:restriction>
1975           </xs:simpleType>
1976         </xs:attribute>
1977         <xs:attribute name="DeviceInHand" use="required">
1978           <xs:simpleType>
1979             <xs:restriction base="xs:NMTOKEN">
1980               <xs:enumeration value="true"/>
1981             </xs:restriction>
1982           </xs:simpleType>
1983         </xs:attribute>
1984       </xs:restriction>
1985     </xs:complexContent>
1986   </xs:complexType>
1987 </xs:schema>
1988
1989
```

1990 **5.3. Authentication Context Classes Extensibility**

1991 As did the core Authentication Context Statement schema, the separate Authentication Context Classes schemas allow
1992 the <Extension> element in certain locations of the tree structure. In general, where the <Extension> element occurred
1993 as a child of a <Choice> element, this option was removed in creating the appropriate class schema definition as an
1994 extension of the base type. When the <Extension> element occurred as an optional child of a <Sequence> element,
1995 the <Extension> element was allowed to remain in addition to any required elements.

1996 Consequently, authentication context statements can include the <Extension> element (with additional elements in
1997 different namespaces) and still conform to authentication context class schemas (if they meet the other requirements
1998 of the schema of course)

1999 The Authentication Context Class schemas extend (as restrictions) appropriate type definitions in the core Authentica-
2000 tion Context Statement schema. As an extension point, the Authentication Context Classes schemas themselves can be
2001 extended - their type definitions serving as base types in some other schema (potentially defined by some community
2002 wishing a more tightly defined authentication context class). To prevent logical inconsistencies, any such extensions
2003 can only further constrain the type definitions of the core Authentication Context Statement schema. To enforce this
2004 constraint, the Authentication Context Class schemas are defined with the finalDefault="extension" attribute on the
2005 <schema> element to prevent this type of extension derivation.

2006 **5.4. Authentication Context Classes Processing Rules**

2007 The processing rules for both Service and Identity Provider for Authentication Context Classes are listed in [LibProt].

2008 **References**

2009 **References**

- 2010 [RFC2119] Bradner, S., eds. (March 1997). Internet Engineering Task Force, "Key words for use in RFCs to Indicate
2011 Requirement Levels," RFC 2119., " <http://www.rfc-editor.org/rfc/rfc2119.txt>,