



Liberty ID-FF Authentication Context Specification

Version: 2.0-01

Editors:

Paul Madsen, Entrust, Inc.

Contributors:

Robert Aarts, Nokia Corporation
Nick Bone, Vodafone Group Plc
Scott Cantor, Internet2, The Ohio State University
Bronislav Kavsan, RSA Security Inc.
John Kemp, Nokia Corporation
Michael Meyerstein, Vodafone Group Plc
Xavier Serret, Gemplus SA

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: draft-liberty-authentication-context-v2.0-01.pdf

1 **Notice**

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

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

15 Copyright © 2004 ActivCard; America Online, Inc.; American Express Travel Related Services; Axalto; Bank of
16 America Corporation; Bell Canada; Cingular Wireless; Cisco Systems, Inc.; Communicator, Inc.; Deloitte & Touche
17 LLP; Earthlink, Inc.; Electronic Data Systems, Inc.; Entrust, Inc.; Epok, Inc.; Ericsson; Fidelity Investments; France
18 Telecom; Gemplus; General Motors; Hewlett-Packard Company; i2 Technologies, Inc.; Internet2; Intuit Inc.;
19 MasterCard International; NEC Corporation; Netegrity, Inc.; NeuStar, Inc.; Nextel Communications; Nippon
20 Telegraph and Telephone Corporation; Nokia Corporation; Novell, Inc.; NTT DoCoMo, Inc.; OneName Corporation;
21 Openwave Systems Inc.; Phaos Technology; Ping Identity Corporation; PricewaterhouseCoopers LLP; RegistryPro,
22 Inc.; RSA Security Inc; Sabre Holdings Corporation; SAP AG; SchlumbergerSema; Sigaba; SK Telecom; Sony
23 Corporation; Sun Microsystems, Inc.; Symlabs, Inc.; Trustgenix; United Airlines; VeriSign, Inc.; Visa International;
24 Vodafone Group Plc; Wave Systems. All rights reserved.

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

31 **Contents**

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

38 1. About this Document

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

41 1.1. Notation and Terminology

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

45 1.1.1. Notational Conventions

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

48 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",
49 "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119](#).

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

53 Listings of XML schemas appear like this.

```
54 <?xml version="1.0" encoding="UTF-8"?>  
55 <xs:schema targetNamespace="urn:liberty:ac:2003-08"  
56     xmlns:xs="http://www.w3.org/2001/XMLSchema"  
57     xmlns="urn:liberty:ac:2003-08">  
58  
59     <!-- Add Stuff Here -->  
60  
61 </xs:schema>  
62
```

63 1.1.2. Namespaces

64 The following namespaces are referred to in this document:

65 **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

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

68 **2. Overview**

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

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

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

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

85 **3. Authentication Context**

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

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

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

97 4. Authentication Context Statement

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

101 4.1. Authentication Context Statement Data Model

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

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

116 4.2. Authentication Context Statement Schema

117 This section lists the complete Authentication Context XML Schema.

```
118
119 <?xml version="1.0" encoding="UTF-8"?>
120 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
121   xmlns:xs="http://www.w3.org/2001/XMLSchema"
122   xmlns="urn:liberty:ac:2003-08">
123
124   <!-- added to get the Extension element -->
125   <xs:include schemaLocation="liberty-utility-v1.0.xsd"/>
126
127   <xs:annotation>
128     <xs:documentation> ### IMPORTANT NOTICE ###
129
130     The source code in this XSD file was excerpted verbatim from:
131
132     Liberty Authentication Context Specification
133     Version 1.2-errata-v1.0
134     12 September 2004
135
136     Copyright (c) 2004 Liberty Alliance participants, see
137     http://www.projectliberty.org/specs/idff_copyrights.html
138   </xs:documentation>
139 </xs:annotation>
140 <xs:element name="AuthenticationContextStatement" type="AuthenticationContextStatementType">
141   <xs:annotation>
142     <xs:documentation>
143       A particular assertion on an identity
144       provider's part with respect to the authentication
```

```

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

```



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

```

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

```

```

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

```

```

413         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
414     </xs:sequence>
415 </xs:complexType>
416 </xs:element>
417
418 <xs:element name="IPAddress">
419     <xs:annotation>
420         <xs:documentation>
421             This element indicates that the Principal has been authenticated through connection from
422 a particular IP address.
423         </xs:documentation>
424     </xs:annotation>
425     <xs:complexType>
426         <xs:sequence>
427             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
428         </xs:sequence>
429     </xs:complexType>
430 </xs:element>
431
432 <xs:element name="AsymmetricDecryption">
433     <xs:annotation>
434         <xs:documentation>
435             The local system has a private key but it is used in decryption mode, rather than
436 signature mode. For example, the Authentication Authority generates a secret and encrypts it using
437 the local system's public key: the local system then proves it has decrypted the secret.
438         </xs:documentation>
439     </xs:annotation>
440     <xs:complexType>
441         <xs:sequence>
442             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
443         </xs:sequence>
444     </xs:complexType>
445 </xs:element>
446
447 <xs:element name="AsymmetricKeyAgreement">
448     <xs:annotation>
449         <xs:documentation>
450             The local system has a private key and uses it for shared secret key agreement with
451 the Authentication Authority (e.g. via Diffie Helman).
452         </xs:documentation>
453     </xs:annotation>
454     <xs:complexType>
455         <xs:sequence>
456             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
457         </xs:sequence>
458     </xs:complexType>
459 </xs:element>
460
461 <xs:element name="SharedSecretDynamicPlaintext">
462     <xs:annotation>
463         <xs:documentation>
464             The local system and Authentication Authority share a secret key. The local system
465 uses this to encrypt a randomized string to pass to the Authentication Authority.
466         </xs:documentation>
467     </xs:annotation>
468     <xs:complexType>
469         <xs:sequence>
470             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
471         </xs:sequence>
472     </xs:complexType>
473 </xs:element>
474
475 <xs:element name="AuthenticatorTransportProtocol" type="AuthenticatorTransportProtocolType">
476     <xs:annotation>
477         <xs:documentation>
478             The protocol across which Authenticator information is transferred to an Authentication
479 Authority verifier.

```

```

480         </xs:documentation>
481     </xs:annotation>
482 </xs:element>
483 <xs:element name="HTTP">
484     <xs:annotation>
485         <xs:documentation>
486             This element indicates that the Authenticator has been transmitted using bare HTTP,
487 utilizing no additional security protocols.
488         </xs:documentation>
489     </xs:annotation>
490     <xs:complexType>
491         <xs:sequence>
492             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
493         </xs:sequence>
494     </xs:complexType>
495 </xs:element>
496 <xs:element name="IPSec">
497     <xs:annotation>
498         <xs:documentation>
499             This element indicates that the Authenticator has been transmitted using a transport
500 mechanism protected by an IPSEC session.
501         </xs:documentation>
502     </xs:annotation>
503     <xs:complexType>
504         <xs:sequence>
505             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
506         </xs:sequence>
507     </xs:complexType>
508 </xs:element>
509 <xs:element name="WTLS">
510     <xs:annotation>
511         <xs:documentation>
512             This element indicates that the Authenticator has been transmitted using a transport
513 mechanism protected by a WTLS session.
514         </xs:documentation>
515     </xs:annotation>
516     <xs:complexType>
517         <xs:sequence>
518             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
519         </xs:sequence>
520     </xs:complexType>
521 </xs:element>
522 <xs:element name="MobileNetworkNoEncryption">
523     <xs:annotation>
524         <xs:documentation>
525             This element indicates that the Authenticator has been transmitted solely across a
526 mobile network using no additional security mechanism.
527         </xs:documentation>
528     </xs:annotation>
529     <xs:complexType>
530         <xs:sequence>
531             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
532         </xs:sequence>
533     </xs:complexType>
534 </xs:element>
535 <xs:element name="MobileNetworkRadioEncryption">
536     <xs:complexType>
537         <xs:sequence>
538             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
539         </xs:sequence>
540     </xs:complexType>
541 </xs:element>
542 <xs:element name="MobileNetworkEndToEndEncryption">
543     <xs:complexType>
544         <xs:sequence>
545             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
546         </xs:sequence>

```

```
547     </xs:complexType>
548 </xs:element>
549
550 <xs:element name="SSL">
551   <xs:annotation>
552     <xs:documentation>
553       This element indicates that the Authenticator has been transmitted using a transport_
554 mechanism protected by an SSL or TLS session.
555     </xs:documentation>
556   </xs:annotation>
557   <xs:complexType>
558     <xs:sequence>
559       <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
560     </xs:sequence>
561   </xs:complexType>
562 </xs:element>
563 <xs:element name="OperationalProtection" type="OperationalProtectionType">
564   <xs:annotation>
565     <xs:documentation>
566       Refers to those characteristics that describe procedural security controls employed by_
567 the Authentication Authority.
568     </xs:documentation>
569   </xs:annotation>
570 </xs:element>
571 <xs:element name="SecurityAudit" type="SecurityAuditType" />
572 <xs:element name="SwitchAudit">
573   <xs:complexType>
574     <xs:sequence>
575       <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
576     </xs:sequence>
577   </xs:complexType>
578 </xs:element>
579 <xs:element name="DeactivationCallCenter">
580   <xs:complexType>
581     <xs:sequence>
582       <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
583     </xs:sequence>
584   </xs:complexType>
585 </xs:element>
586 <xs:element name="GoverningAgreements" type="GoverningAgreementsType">
587   <xs:annotation>
588     <xs:documentation>
589       Provides a mechanism for linking to external (likely human readable) documents in which_
590 additional business agreements, (e.g. liability constraints, obligations, etc) can be placed.
591     </xs:documentation>
592   </xs:annotation>
593 </xs:element>
594 <xs:element name="GoverningAgreementRef" type="GoverningAgreementRefType" />
595 <xs:element name="AuthenticatingAuthority" type="AuthenticatingAuthorityType">
596   <xs:annotation>
597     <xs:documentation>
598       The Authority that originally authenticated the Principal.
599     </xs:documentation>
600   </xs:annotation>
601 </xs:element>
602 <xs:complexType name="IdentificationType">
603   <xs:sequence>
604     <xs:element ref="PhysicalVerification" minOccurs="0" />
605     <xs:element ref="WrittenConsent" minOccurs="0" />
606     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
607   </xs:sequence>
608   <xs:attribute name="nym">
609     <xs:annotation>
610       <xs:documentation>
611         This attribute indicates whether or not the Identification mechanisms allow the_
612 actions of the Principal to be linked to an actual end user.
613       </xs:documentation>

```

```

614         </xs:annotation>
615         <xs:simpleType>
616             <xs:restriction base="xs:NMTOKEN">
617                 <xs:enumeration value="anonymity" />
618                 <xs:enumeration value="verinymity" />
619                 <xs:enumeration value="pseudonymity" />
620             </xs:restriction>
621         </xs:simpleType>
622     </xs:attribute>
623 </xs:complexType>
624 <xs:complexType name="GoverningAgreementsType">
625     <xs:sequence>
626         <xs:element ref="GoverningAgreementRef" maxOccurs="unbounded" />
627     </xs:sequence>
628 </xs:complexType>
629 <xs:complexType name="GoverningAgreementRefType">
630     <xs:attribute name="governingAgreementRef" type="xs:anyURI" use="required" />
631 </xs:complexType>
632 <xs:complexType name="AuthenticatingAuthorityType">
633     <xs:sequence>
634         <xs:element ref="GoverningAgreements" />
635     </xs:sequence>
636     <xs:attribute name="ID" type="xs:anyURI" use="required" />
637 </xs:complexType>
638 <xs:complexType name="AuthenticatorTransportProtocolType">
639     <xs:choice>
640         <xs:element ref="HTTP" />
641         <xs:element ref="SSL" />
642         <xs:element ref="MobileNetworkNoEncryption" />
643         <xs:element ref="MobileNetworkRadioEncryption" />
644         <xs:element ref="MobileNetworkEndToEndEncryption" />
645         <xs:element ref="WTLS" />
646         <xs:element ref="IPSec" />
647         <xs:element ref="Extension" maxOccurs="unbounded" />
648     </xs:choice>
649 </xs:complexType>
650 <xs:complexType name="PrincipalAuthenticationMechanismType">
651     <xs:choice>
652         <xs:element ref="Password" />
653         <xs:element ref="Token" />
654         <xs:element ref="Smartcard" />
655         <xs:element ref="ActivationPin" />
656         <xs:element ref="Extension" maxOccurs="unbounded" />
657     </xs:choice>
658 </xs:complexType>
659 <xs:complexType name="AuthenticationMethodType">
660     <xs:sequence>
661         <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0" />
662         <xs:element ref="Authenticator" minOccurs="0" />
663         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0" />
664         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
665     </xs:sequence>
666 </xs:complexType>
667 <xs:complexType name="AuthenticationContextStatement Type">
668     <xs:sequence>
669         <xs:element ref="Identification" minOccurs="0" />
670         <xs:element ref="TechnicalProtection" minOccurs="0" />
671         <xs:element ref="OperationalProtection" minOccurs="0" />
672         <xs:element ref="AuthenticationMethod" minOccurs="0" />
673         <xs:element ref="GoverningAgreements" minOccurs="0" />
674         <xs:element ref="AuthenticatingAuthority" minOccurs="0" maxOccurs="unbounded" />
675         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
676     </xs:sequence>
677     <xs:attribute name="ID" type="xs:ID" />
678 </xs:complexType>
679 <xs:complexType name="TechnicalProtectionType">
680     <xs:choice>
    
```



```

681         <xs:element ref="PrivateKeyProtection" minOccurs="0"/>
682         <xs:element ref="SecretKeyProtection" minOccurs="0"/>
683         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
684     </xs:choice>
685 </xs:complexType>
686 <xs:complexType name="OperationalProtectionType">
687     <xs:sequence>
688         <xs:element ref="SecurityAudit" minOccurs="0"/>
689         <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
690         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
691     </xs:sequence>
692 </xs:complexType>
693 <xs:complexType name="AuthenticatorType">
694     <xs:choice>
695         <xs:element ref="PreviousSession"/>
696         <xs:element ref="ResumeSession"/>
697         <xs:element ref="DigSig"/>
698         <xs:element ref="Password"/>
699         <xs:element ref="ZeroKnowledge"/>
700         <xs:element ref="SharedSecretChallengeResponse"/>
701         <xs:element ref="SharedSecretDynamicPlaintext"/>
702         <xs:element ref="IPAddress"/>
703     <xs:element ref="AsymmetricDecryption"/>
704     <xs:element ref="AsymmetricKeyAgreement"/>
705         <xs:element ref="Extension" maxOccurs="unbounded"/>
706     </xs:choice>
707 </xs:complexType>
708 <xs:complexType name="KeyActivationType">
709     <xs:choice>
710         <xs:element ref="ActivationPin"/>
711         <xs:element ref="Extension" maxOccurs="unbounded"/>
712     </xs:choice>
713 </xs:complexType>
714 <xs:complexType name="KeySharingType">
715     <xs:attribute name="sharing" type="xs:boolean" use="required"/>
716 </xs:complexType>
717 <xs:complexType name="PrivateKeyProtectionType">
718     <xs:sequence>
719         <xs:element ref="KeyActivation" minOccurs="0"/>
720         <xs:element ref="KeyStorage" minOccurs="0"/>
721         <xs:element ref="KeySharing" minOccurs="0"/>
722         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
723     </xs:sequence>
724 </xs:complexType>
725
726 <xs:complexType name="PasswordType">
727     <xs:sequence>
728         <xs:element ref="Length" minOccurs="0"/>
729         <xs:element ref="Alphabet" minOccurs="0"/>
730         <xs:element ref="Generation" minOccurs="0"/>
731         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
732     </xs:sequence>
733 </xs:complexType>
734
735 <xs:complexType name="ActivationPinType">
736     <xs:sequence>
737         <xs:element ref="Length" minOccurs="0"/>
738         <xs:element ref="Alphabet" minOccurs="0"/>
739         <xs:element ref="Generation" minOccurs="0"/>
740         <xs:element ref="ActivationLimit" minOccurs="0"/>
741         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
742     </xs:sequence>
743 </xs:complexType>
744
745 <xs:element name="Alphabet" type="AlphabetType"/>
746
747 <xs:complexType name="AlphabetType">

```



```

748     <xs:attribute name="requiredChars" type="xs:string" use="required"/>
749     <xs:attribute name="excludedChars" type="xs:string" use="optional"/>
750     <xs:attribute name="case" type="xs:string" use="optional"/>
751 </xs:complexType>
752
753 <xs:complexType name="TokenType">
754   <xs:sequence>
755     <xs:element ref="TimeSyncToken"/>
756     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
757   </xs:sequence>
758 </xs:complexType>
759 <xs:complexType name="TimeSyncTokenType">
760   <xs:attribute name="DeviceType" use="required">
761     <xs:simpleType>
762       <xs:restriction base="xs:NMTOKEN">
763         <xs:enumeration value="hardware"/>
764         <xs:enumeration value="software"/>
765       </xs:restriction>
766     </xs:simpleType>
767   </xs:attribute>
768   <xs:attribute name="SeedLength" type="xs:integer" use="required"/>
769   <xs:attribute name="DeviceInHand" use="required">
770     <xs:simpleType>
771       <xs:restriction base="xs:NMTOKEN">
772         <xs:enumeration value="true"/>
773         <xs:enumeration value="false"/>
774       </xs:restriction>
775     </xs:simpleType>
776   </xs:attribute>
777 </xs:complexType>
778 <xs:complexType name="ActivationLimitType">
779   <xs:choice>
780     <xs:element ref="ActivationLimitDuration"/>
781     <xs:element ref="ActivationLimitUsages"/>
782     <xs:element ref="ActivationLimitSession"/>
783   </xs:choice>
784 </xs:complexType>
785
786 <xs:element name="ActivationLimitDuration" type="ActivationLimitDurationType">
787   <xs:annotation>
788     <xs:documentation>
789       This element indicates that the Key Activation Limit is defined
790       as a specific duration of time.
791     </xs:documentation>
792   </xs:annotation>
793 </xs:element>
794
795 <xs:element name="ActivationLimitUsages" type="ActivationLimitUsagesType">
796   <xs:annotation>
797     <xs:documentation>
798       This element indicates that the Key Activation Limit is defined as a number of usages.
799     </xs:documentation>
800   </xs:annotation>
801 </xs:element>
802
803 <xs:element name="ActivationLimitSession" type="ActivationLimitSessionType">
804   <xs:annotation>
805     <xs:documentation>
806       This element indicates that the Key Activation Limit is the session.
807     </xs:documentation>
808   </xs:annotation>
809 </xs:element>
810
811 <xs:complexType name="ActivationLimitDurationType">
812   <xs:attribute name="duration" type="xs:duration" use="required"/>
813 </xs:complexType>
814

```

```
815     <xs:complexType name="ActivationLimitUsagesType">
816       <xs:attribute name="number" type="xs:integer" use="required"/>
817     </xs:complexType>
818
819     <xs:complexType name="ActivationLimitSessionType"/>
820
821     <xs:complexType name="LengthType">
822       <xs:attribute name="min" type="xs:integer" use="required"/>
823       <xs:attribute name="max" type="xs:integer" use="optional"/>
824     </xs:complexType>
825
826     <xs:complexType name="KeyStorageType">
827       <xs:attribute name="medium" use="required">
828         <xs:simpleType>
829           <xs:restriction base="xs:NMTOKEN">
830             <xs:enumeration value="memory"/>
831             <xs:enumeration value="smartcard"/>
832             <xs:enumeration value="token"/>
833             <xs:enumeration value="MobileDevice"/>
834             <xs:enumeration value="MobileAuthCard"/>
835           </xs:restriction>
836         </xs:simpleType>
837       </xs:attribute>
838     </xs:complexType>
839     <xs:complexType name="SecretKeyProtectionType">
840       <xs:sequence>
841         <xs:element ref="KeyActivation" minOccurs="0"/>
842         <xs:element ref="KeyStorage" minOccurs="0"/>
843         <xs:element ref="Extension" maxOccurs="unbounded"/>
844       </xs:sequence>
845     </xs:complexType>
846     <xs:complexType name="SecurityAuditType">
847       <xs:sequence>
848         <xs:element ref="SwitchAudit" minOccurs="0"/>
849         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
850       </xs:sequence>
851     </xs:complexType>
852 </xs:schema>
853
854
```

855 4.3. Authentication Context Statement Extensibility

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

861 4.4. Authentication Context Statement Processing Rules

862 The processing rules for Authentication Context Statements are listed in [\[LibertyProtSchema\]](#).

863 **5. Authentication Context Classes**

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

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

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

887 **5.1. Advantages of Authentication Context Classes**

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

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

898 **5.2. Authentication Context Class Schemas**

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

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

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

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

905 **5.2.1. Internet Protocol**

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

907 **5.2.1.1. Associated Liberty URI**

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

909 **5.2.1.2. Class Schema**

```
910
911 <?xml version="1.0" encoding="UTF-8"?>
912 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
913   xmlns:xs="http://www.w3.org/2001/XMLSchema"
914   xmlns="urn:liberty:ac:2003-08"
915   version="1.2-08" finalDefault="extension">
916   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
917   <xs:annotation>
918     <xs:documentation>
919       http://www.projectliberty.org/schemas/authctx/classes/InternetProtocol</x
920 s:documentation>
921   </xs:annotation>
922   <xs:complexType name="InternetProtocolAuthenticatorType">
923     <xs:complexContent>
924       <xs:restriction base="AuthenticatorType">
925         <xs:choice>
926           <xs:element ref="IPAddress"/>
927         </xs:choice>
928       </xs:restriction>
929     </xs:complexContent>
930   </xs:complexType>
931 </xs:schema>
932
933
```

934 **5.2.2. InternetProtocolPassword**

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

937 **5.2.2.1. Associated Liberty URI**

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

939 **5.2.2.2. Class Schema**

```
940
941 <?xml version="1.0" encoding="UTF-8"?>
942 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
943   xmlns="urn:liberty:ac:2003-08"
```

```

944   xmlns:xs="http://www.w3.org/2001/XMLSchema"
945   version="1.2-08" finalDefault="extension">
946   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
947   <xs:annotation>
948     <xs:documentation>
949       http://www.projectliberty.org/schemas/authctx/classes/InternetProtocolPas
950 sword</xs:documentation>
951   </xs:annotation>
952
953   <xs:complexType name="InternetProtocolPasswordType">
954     <xs:complexContent>
955       <xs:restriction base="PasswordType">
956         <xs:sequence>
957           <xs:element ref="Length"/>
958           <xs:element ref="Generation" minOccurs="0"/>
959           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
960         </xs:sequence>
961       </xs:restriction>
962     </xs:complexContent>
963   </xs:complexType>
964   <xs:complexType name="InternetProtocolPasswordLengthType">
965     <xs:complexContent>
966       <xs:restriction base="LengthType">
967         <xs:attribute name="min" use="required">
968           <xs:simpleType>
969             <xs:restriction base="xs:integer">
970               <xs:minInclusive value="3"/>
971             </xs:restriction>
972           </xs:simpleType>
973         </xs:attribute>
974         <xs:attribute name="max" type="xs:integer" use="optional"/>
975       </xs:restriction>
976     </xs:complexContent>
977   </xs:complexType>
978   <xs:complexType name="InternetProtocolPasswordAuthenticatorType">
979     <xs:complexContent>
980       <xs:restriction base="AuthenticatorType">
981         <xs:sequence>
982           <xs:element ref="IPAddress"/>
983           <xs:element ref="Password"/>
984           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
985         </xs:sequence>
986       </xs:restriction>
987     </xs:complexContent>
988   </xs:complexType>
989 </xs:schema>
990
991

```

992 5.2.3. MobileOneFactorUnregistered

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

996 5.2.3.1. Associated Liberty URI

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

998 5.2.3.2. Class Schema

```

999
1000 <?xml version="1.0" encoding="UTF-8"?>
1001 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1002   xmlns="urn:liberty:ac:2003-08"

```

```

1003     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1004     finalDefault="extension" version="1.2-08">
1005     <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1006     <xs:annotation>
1007       <xs:documentation>http://www.projectliberty.org/schemas/authctx/classes/Mo
1008     bileOneFactorUnregistered</xs:documentation>
1009     </xs:annotation>
1010     <xs:complexType name="MobileOneFactorUnregisteredAuthenticatorType">
1011       <xs:complexContent>
1012         <xs:restriction base="AuthenticatorType">
1013           <xs:choice>
1014             <xs:element ref="DigSig"/>
1015             <xs:element ref="ZeroKnowledge"/>
1016             <xs:element ref="SharedSecretChallengeResponse"/>
1017             <xs:element ref="AsymmetricDecryption"/>
1018             <xs:element ref="AsymmetricKeyAgreement"/>
1019             <xs:element ref="SharedSecretDynamicPlaintext"/>
1020           </xs:choice>
1021         </xs:restriction>
1022       </xs:complexContent>
1023     </xs:complexType>
1024     <xs:complexType name="MobileOneFactorUnregisteredAuthenticatorTransportProtocolType">
1025       <xs:complexContent>
1026         <xs:restriction base="AuthenticatorTransportProtocolType">
1027           <xs:choice>
1028             <xs:element ref="MobileNetworkNoEncryption"/>
1029             <xs:element ref="MobileNetworkRadioEncryption"/>
1030             <xs:element ref="MobileNetworkEndToEndEncryption"/>
1031             <xs:element ref="WTLS"/>
1032           </xs:choice>
1033         </xs:restriction>
1034       </xs:complexContent>
1035     </xs:complexType>
1036     <xs:complexType name="MobileOneFactorUnregisteredOperationalProtectionType">
1037       <xs:complexContent>
1038         <xs:restriction base="OperationalProtectionType">
1039           <xs:sequence>
1040             <xs:element ref="SecurityAudit"/>
1041             <xs:element ref="DeactivationCallCenter"/>
1042             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1043           </xs:sequence>
1044         </xs:restriction>
1045       </xs:complexContent>
1046     </xs:complexType>
1047     <xs:complexType name="MobileOneFactorUnregisteredTechnicalProtectionType">
1048       <xs:complexContent>
1049         <xs:restriction base="TechnicalProtectionType">
1050           <xs:choice>
1051             <xs:element ref="PrivateKeyProtection"/>
1052             <xs:element ref="SecretKeyProtection"/>
1053           </xs:choice>
1054         </xs:restriction>
1055       </xs:complexContent>
1056     </xs:complexType>
1057     <xs:complexType name="MobileOneFactorUnregisteredPrivateKeyProtectionType">
1058       <xs:complexContent>
1059         <xs:restriction base="PrivateKeyProtectionType">
1060           <xs:sequence>
1061             <xs:element ref="KeyStorage"/>
1062             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1063           </xs:sequence>
1064         </xs:restriction>
1065       </xs:complexContent>
1066     </xs:complexType>
1067     <xs:complexType name="MobileOneFactorUnregisteredSecretKeyProtectionType">
1068       <xs:complexContent>
1069         <xs:restriction base="SecretKeyProtectionType">

```

```

1070         <xs:sequence>
1071             <xs:element ref="KeyStorage" />
1072             <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1073         </xs:sequence>
1074     </xs:restriction>
1075 </xs:complexContent>
1076 </xs:complexType>
1077 <xs:complexType name="MobileOneFactorUnregisteredKeyStorageType">
1078     <xs:complexContent>
1079         <xs:restriction base="KeyStorageType">
1080             <xs:attribute name="medium" use="required">
1081                 <xs:simpleType>
1082                     <xs:restriction base="xs:NMTOKEN">
1083                         <xs:enumeration value="MobileDevice" />
1084                         <xs:enumeration value="MobileAuthCard" />
1085                         <xs:enumeration value="smartcard" />
1086                     </xs:restriction>
1087                 </xs:simpleType>
1088             </xs:attribute>
1089         </xs:restriction>
1090     </xs:complexContent>
1091 </xs:complexType>
1092 <xs:complexType name="MobileOneFactorUnregisteredSecurityAuditType">
1093     <xs:complexContent>
1094         <xs:restriction base="SecurityAuditType">
1095             <xs:sequence>
1096                 <xs:element ref="SwitchAudit" />
1097                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1098             </xs:sequence>
1099         </xs:restriction>
1100     </xs:complexContent>
1101 </xs:complexType>
1102 <xs:complexType name="MobileOneFactorUnregisteredIdentificationType">
1103     <xs:complexContent>
1104         <xs:restriction base="IdentificationType">
1105             <xs:attribute name="nym">
1106                 <xs:simpleType>
1107                     <xs:restriction base="xs:NMTOKEN">
1108                         <xs:enumeration value="anonymity" />
1109                         <xs:enumeration value="pseudonymity" />
1110                     </xs:restriction>
1111                 </xs:simpleType>
1112             </xs:attribute>
1113         </xs:restriction>
1114     </xs:complexContent>
1115 </xs:complexType>
1116 </xs:schema>
1117
1118
    
```

1119 5.2.4. MobileTwoFactorUnregistered

1120 Reflects no mobile customer registration procedures and a two-factor based authentication, such as secure device and
 1121 user PIN. This context class is useful when a service other than the mobile operator wants to link their customer ID
 1122 to a mobile supplied two-factor authentication service by capturing mobile phone data at enrollment.

1123 5.2.4.1. Associated Liberty URI

1124 <http://www.projectliberty.org/schemas/authctx/classes/MobileTwoFactorUnregistered>

1125 5.2.4.2. Class Schema

```

1126
1127 <?xml version="1.0" encoding="UTF-8"?>
1128 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
    
```

```
1129 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1130 xmlns="urn:liberty:ac:2003-08"
1131 version="1.2-08"
1132 finalDefault="extension">
1133 <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1134 <xs:annotation>
1135   <xs:documentation>
1136     http://www.projectliberty.org/schemas/authctx/classes/MobileTwoFactorUnregistered
1137   </xs:documentation>
1138 </xs:annotation>
1139
1140 <xs:complexType name="MobileTwoFactorUnregisteredAuthenticatorType">
1141   <xs:complexContent>
1142     <xs:restriction base="AuthenticatorType">
1143       <xs:choice>
1144         <xs:element ref="DigSig"/>
1145         <xs:element ref="ZeroKnowledge"/>
1146         <xs:element ref="SharedSecretChallengeResponse"/>
1147         <xs:element ref="AsymmetricDecryption"/>
1148         <xs:element ref="AsymmetricKeyAgreement"/>
1149         <xs:element ref="SharedSecretDynamicPlaintext"/>
1150         <xs:sequence>
1151           <xs:element ref="Password" minOccurs="1"/>
1152           <xs:choice>
1153             <xs:element ref="SharedSecretDynamicPlaintext"/>
1154             <xs:element ref="SharedSecretChallengeResponse"/>
1155           </xs:choice>
1156           <xs:element ref="Extension" maxOccurs="unbounded"/>
1157         </xs:sequence>
1158       </xs:choice>
1159     </xs:restriction>
1160   </xs:complexContent>
1161 </xs:complexType>
1162 <xs:complexType name="MobileTwoFactorUnregisteredAuthenticatorTransportProtocolType">
1163   <xs:complexContent>
1164     <xs:restriction base="AuthenticatorTransportProtocolType">
1165       <xs:choice>
1166         <xs:element ref="MobileNetworkNoEncryption"/>
1167         <xs:element ref="MobileNetworkRadioEncryption"/>
1168         <xs:element ref="MobileNetworkEndToEndEncryption"/>
1169         <xs:element ref="WTLS"/>
1170       </xs:choice>
1171     </xs:restriction>
1172   </xs:complexContent>
1173 </xs:complexType>
1174 <xs:complexType name="MobileTwoFactorUnregisteredOperationalProtectionType">
1175   <xs:complexContent>
1176     <xs:restriction base="OperationalProtectionType">
1177       <xs:sequence>
1178         <xs:element ref="SecurityAudit"/>
1179         <xs:element ref="DeactivationCallCenter"/>
1180         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1181       </xs:sequence>
1182     </xs:restriction>
1183   </xs:complexContent>
1184 </xs:complexType>
1185 <xs:complexType name="MobileTwoFactorUnregisteredTechnicalProtectionType">
1186   <xs:complexContent>
1187     <xs:restriction base="TechnicalProtectionType">
1188       <xs:choice>
1189         <xs:element ref="PrivateKeyProtection"/>
1190         <xs:element ref="SecretKeyProtection"/>
1191       </xs:choice>
1192     </xs:restriction>
1193   </xs:complexContent>
1194 </xs:complexType>
1195
```



```

1196 <xs:complexType name="MobileTwoFactorUnregisteredPrivateKeyProtectionType">
1197   <xs:complexContent>
1198     <xs:restriction base="PrivateKeyProtectionType">
1199       <xs:sequence>
1200         <xs:element ref="KeyActivation" minOccurs="1" maxOccurs="1"/>
1201         <xs:element ref="KeyStorage" minOccurs="0"/>
1202         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1203       </xs:sequence>
1204     </xs:restriction>
1205   </xs:complexContent>
1206 </xs:complexType>
1207
1208 <xs:complexType name="MobileTwoFactorUnregisteredSecretKeyProtectionType">
1209   <xs:complexContent>
1210     <xs:restriction base="SecretKeyProtectionType">
1211       <xs:sequence>
1212         <xs:element ref="KeyActivation"/>
1213         <xs:element ref="KeyStorage"/>
1214         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1215       </xs:sequence>
1216     </xs:restriction>
1217   </xs:complexContent>
1218 </xs:complexType>
1219
1220 <xs:complexType name="MobileTwoFactorUnregisteredKeyActivationType">
1221   <xs:complexContent>
1222     <xs:restriction base="KeyActivationType">
1223       <xs:sequence>
1224         <xs:element ref="ActivationPin"/>
1225         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1226       </xs:sequence>
1227     </xs:restriction>
1228   </xs:complexContent>
1229 </xs:complexType>
1230
1231 <xs:complexType name="MobileTwoFactorUnregisteredKeyStorageType">
1232   <xs:complexContent>
1233     <xs:restriction base="KeyStorageType">
1234       <xs:attribute name="medium" use="required">
1235         <xs:simpleType>
1236           <xs:restriction base="xs:NMTOKEN">
1237             <xs:enumeration value="MobileDevice"/>
1238             <xs:enumeration value="MobileAuthCard"/>
1239             <xs:enumeration value="smartcard"/>
1240           </xs:restriction>
1241         </xs:simpleType>
1242       </xs:attribute>
1243     </xs:restriction>
1244   </xs:complexContent>
1245 </xs:complexType>
1246
1247 <xs:complexType name="MobileTwoFactorUnregisteredSecurityAuditType">
1248   <xs:complexContent>
1249     <xs:restriction base="SecurityAuditType">
1250       <xs:sequence>
1251         <xs:element ref="SwitchAudit"/>
1252         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1253       </xs:sequence>
1254     </xs:restriction>
1255   </xs:complexContent>
1256 </xs:complexType>
1257
1258 <xs:complexType name="MobileTwoFactorUnregisteredIdentificationType">
1259   <xs:complexContent>
1260     <xs:restriction base="IdentificationType">
1261       <xs:attribute name="nym">
1262         <xs:simpleType>

```

```

1263         <xs:restriction base="xs:NMTOKEN">
1264             <xs:enumeration value="anonymity"/>
1265             <xs:enumeration value="pseudonymity"/>
1266         </xs:restriction>
1267     </xs:simpleType>
1268 </xs:attribute>
1269 </xs:restriction>
1270 </xs:complexContent>
1271 </xs:complexType>
1272
1273 </xs:schema>
1274
1275

```

1276 5.2.5. MobileOneFactorContract

1277 Reflects mobile contract customer registration procedures and a single factor authentication. For example, a digital
1278 signing device with tamper resistant memory for key storage, such as the mobile MSISDN, but no required PIN or
1279 biometric for real-time user authentication.

1280 5.2.5.1. Associated Liberty URI

1281 <http://www.projectliberty.org/schemas/authctx/classes/MobileOneFactorContract>

1282 5.2.5.2. Class Schema

```

1283
1284 <?xml version="1.0" encoding="UTF-8"?>
1285 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1286     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1287     xmlns="urn:liberty:ac:2003-08"
1288     version="1.2-08" finalDefault="extension">
1289     <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1290     <xs:annotation>
1291 <xs:documentation>http://www.projectliberty.org/schemas/authctx/classes/MobileOneFa
1292 ctorContract</xs:documentation></xs:annotation>
1293
1294     <xs:complexType name="MobileOneFactorContractAuthenticatorType">
1295         <xs:complexContent>
1296             <xs:restriction base="AuthenticatorType">
1297                 <xs:choice maxOccurs="1">
1298                     <xs:element ref="DigSig"/>
1299                     <xs:element ref="ZeroKnowledge"/>
1300                     <xs:element ref="SharedSecretChallengeResponse"/>
1301                     <xs:element ref="AsymmetricDecryption"/>
1302                     <xs:element ref="AsymmetricKeyAgreement"/>
1303                     <xs:element ref="SharedSecretDynamicPlaintext"/>
1304                 </xs:choice>
1305             </xs:restriction>
1306         </xs:complexContent>
1307     </xs:complexType>
1308     <xs:complexType name="MobileOneFactorContractAuthenticatorTransportProtocolType">
1309         <xs:complexContent>
1310             <xs:restriction base="AuthenticatorTransportProtocolType">
1311                 <xs:choice>
1312                     <xs:element ref="MobileNetworkNoEncryption"/>
1313                     <xs:element ref="MobileNetworkRadioEncryption"/>
1314                     <xs:element ref="MobileNetworkEndToEndEncryption"/>
1315                     <xs:element ref="WTLS"/>
1316                 </xs:choice>
1317             </xs:restriction>
1318         </xs:complexContent>
1319     </xs:complexType>
1320     <xs:complexType name="MobileOneFactorContractOperationalProtectionType">
1321         <xs:complexContent>

```

```
1322     <xs:restriction base="OperationalProtectionType">
1323       <xs:sequence>
1324         <xs:element ref="SecurityAudit"/>
1325         <xs:element ref="DeactivationCallCenter"/>
1326         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1327       </xs:sequence>
1328     </xs:restriction>
1329   </xs:complexContent>
1330 </xs:complexType>
1331 <xs:complexType name="MobileOneFactorContractTechnicalProtectionType">
1332   <xs:complexContent>
1333     <xs:restriction base="TechnicalProtectionType">
1334       <xs:choice>
1335         <xs:element ref="PrivateKeyProtection"/>
1336         <xs:element ref="SecretKeyProtection"/>
1337       </xs:choice>
1338     </xs:restriction>
1339   </xs:complexContent>
1340 </xs:complexType>
1341
1342 <xs:complexType name="MobileOneFactorContractPrivateKeyProtectionType">
1343   <xs:complexContent>
1344     <xs:restriction base="PrivateKeyProtectionType">
1345       <xs:sequence maxOccurs="1">
1346         <xs:element ref="KeyStorage"/>
1347         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1348       </xs:sequence>
1349     </xs:restriction>
1350   </xs:complexContent>
1351 </xs:complexType>
1352
1353 <xs:complexType name="MobileOneFactorContractSecretKeyProtectionType">
1354   <xs:complexContent>
1355     <xs:restriction base="SecretKeyProtectionType">
1356       <xs:sequence>
1357         <xs:element ref="KeyStorage"/>
1358         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1359       </xs:sequence>
1360     </xs:restriction>
1361   </xs:complexContent>
1362 </xs:complexType>
1363
1364 <xs:complexType name="MobileOneFactorContractKeyStorageType">
1365   <xs:complexContent>
1366     <xs:restriction base="KeyStorageType">
1367       <xs:attribute name="medium" use="required">
1368         <xs:simpleType>
1369           <xs:restriction base="xs:NMTOKEN">
1370             <xs:enumeration value="MobileDevice"/>
1371             <xs:enumeration value="MobileAuthCard"/>
1372             <xs:enumeration value="smartcard"/>
1373           </xs:restriction>
1374         </xs:simpleType>
1375       </xs:attribute>
1376     </xs:restriction>
1377   </xs:complexContent>
1378 </xs:complexType>
1379
1380 <xs:complexType name="MobileOneFactorContractSecurityAuditType">
1381   <xs:complexContent>
1382     <xs:restriction base="SecurityAuditType">
1383       <xs:sequence>
1384         <xs:element ref="SwitchAudit"/>
1385         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1386       </xs:sequence>
1387     </xs:restriction>
1388   </xs:complexContent>
```

```

1389 </xs:complexType>
1390
1391 <xs:complexType name="MobileOneFactorContractIdentificationType">
1392 <xs:complexContent>
1393 <xs:restriction base="IdentificationType">
1394 <xs:sequence>
1395 <xs:element ref="PhysicalVerification"/>
1396 <xs:element ref="WrittenConsent"/>
1397 <xs:element ref="GoverningAgreements"/>
1398 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1399 </xs:sequence>
1400 <xs:attribute name="nym">
1401 <xs:simpleType>
1402 <xs:restriction base="xs:NMTOKEN">
1403 <xs:enumeration value="anonymity"/>
1404 <xs:enumeration value="verinymity"/>
1405 <xs:enumeration value="pseudonymity"/>
1406 </xs:restriction>
1407 </xs:simpleType>
1408 </xs:attribute>
1409 </xs:restriction>
1410 </xs:complexContent>
1411 </xs:complexType>
1412
1413 </xs:schema>
1414
1415

```

1416 5.2.6. MobileTwoFactorContract

1417 Reflects mobile contract customer registration procedures and a two-factor based authentication. For example, a
 1418 digital signing device with tamper resistant memory for key storage, such as a GSM SIM, that requires explicit proof
 1419 of user identity and intent, such as a PIN or biometric.

1420 5.2.6.1. Associated Liberty URI

1421 <http://www.projectliberty.org/schemas/authctx/classes/MobileTwoFactorContract>

1422 5.2.6.2. Class Schema

```

1423
1424 <?xml version="1.0" encoding="UTF-8"?>
1425 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1426 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1427 xmlns="urn:liberty:ac:2003-08"
1428 version="1.2-08"
1429 finalDefault="extension">
1430 <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1431 <xs:annotation><xs:documentation>http://www.projectliberty.org/schemas/authctx/classes/MobileT
1432 woFactorContract</xs:documentation>
1433 </xs:annotation>
1434
1435 <xs:complexType name="MobileTwoFactorContractAuthenticatorType">
1436 <xs:complexContent>
1437 <xs:restriction base="AuthenticatorType">
1438 <xs:choice>
1439 <xs:element ref="DigSig"/>
1440 <xs:element ref="ZeroKnowledge"/>
1441 <xs:element ref="SharedSecretChallengeResponse"/>
1442 <xs:element ref="AsymmetricDecryption"/>
1443 <xs:element ref="AsymmetricKeyAgreement"/>
1444 <xs:element ref="SharedSecretDynamicPlaintext"/>
1445 <xs:sequence>
1446 <xs:element ref="Password" minOccurs="1"/>
1447 </xs:sequence>

```

```

1448         <xs:element ref="SharedSecretDynamicPlaintext" />
1449         <xs:element ref="SharedSecretChallengeResponse" />
1450     </xs:choice>
1451     <xs:element ref="Extension" maxOccurs="unbounded" />
1452 </xs:sequence>
1453 </xs:choice>
1454 </xs:restriction>
1455 </xs:complexContent>
1456 </xs:complexType>
1457 <xs:complexType name="MobileTwoFactorContractAuthenticatorTransportProtocolType">
1458     <xs:complexContent>
1459         <xs:restriction base="AuthenticatorTransportProtocolType">
1460             <xs:choice>
1461                 <xs:element ref="MobileNetworkNoEncryption" />
1462                 <xs:element ref="MobileNetworkRadioEncryption" />
1463                 <xs:element ref="MobileNetworkEndToEndEncryption" />
1464                 <xs:element ref="WTLS" />
1465             </xs:choice>
1466         </xs:restriction>
1467     </xs:complexContent>
1468 </xs:complexType>
1469 <xs:complexType name="MobileTwoFactorContractOperationalProtectionType">
1470     <xs:complexContent>
1471         <xs:restriction base="OperationalProtectionType">
1472             <xs:sequence>
1473                 <xs:element ref="SecurityAudit" />
1474                 <xs:element ref="DeactivationCallCenter" />
1475                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1476             </xs:sequence>
1477         </xs:restriction>
1478     </xs:complexContent>
1479 </xs:complexType>
1480 <xs:complexType name="MobileTwoFactorContractTechnicalProtectionType">
1481     <xs:complexContent>
1482         <xs:restriction base="TechnicalProtectionType">
1483             <xs:choice>
1484                 <xs:element ref="PrivateKeyProtection" />
1485                 <xs:element ref="SecretKeyProtection" />
1486             </xs:choice>
1487         </xs:restriction>
1488     </xs:complexContent>
1489 </xs:complexType>
1490
1491 <xs:complexType name="MobileTwoFactorContractPrivateKeyProtectionType">
1492     <xs:complexContent>
1493         <xs:restriction base="PrivateKeyProtectionType">
1494             <xs:sequence>
1495                 <xs:element ref="KeyActivation" minOccurs="1" maxOccurs="1" />
1496                 <xs:element ref="KeyStorage" minOccurs="0" />
1497                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1498             </xs:sequence>
1499         </xs:restriction>
1500     </xs:complexContent>
1501 </xs:complexType>
1502
1503 <xs:complexType name="MobileTwoFactorContractSecretKeyProtectionType">
1504     <xs:complexContent>
1505         <xs:restriction base="SecretKeyProtectionType">
1506             <xs:sequence>
1507                 <xs:element ref="KeyActivation" />
1508                 <xs:element ref="KeyStorage" />
1509                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1510             </xs:sequence>
1511         </xs:restriction>
1512     </xs:complexContent>
1513 </xs:complexType>
1514
    
```

```

1515 <xs:complexType name="MobileTwoFactorContractKeyActivationType">
1516 <xs:complexContent>
1517 <xs:restriction base="KeyActivationType">
1518 <xs:sequence>
1519 <xs:element ref="ActivationPin"/>
1520 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1521 </xs:sequence>
1522 </xs:restriction>
1523 </xs:complexContent>
1524 </xs:complexType>
1525
1526 <xs:complexType name="MobileTwoFactorContractKeyStorageType">
1527 <xs:complexContent>
1528 <xs:restriction base="KeyStorageType">
1529 <xs:attribute name="medium" use="required">
1530 <xs:simpleType>
1531 <xs:restriction base="xs:NMTOKEN">
1532 <xs:enumeration value="MobileDevice"/>
1533 <xs:enumeration value="MobileAuthCard"/>
1534 <xs:enumeration value="smartcard"/>
1535 </xs:restriction>
1536 </xs:simpleType>
1537 </xs:attribute>
1538 </xs:restriction>
1539 </xs:complexContent>
1540 </xs:complexType>
1541
1542 <xs:complexType name="MobileTwoFactorContractSecurityAuditType">
1543 <xs:complexContent>
1544 <xs:restriction base="SecurityAuditType">
1545 <xs:sequence>
1546 <xs:element ref="SwitchAudit"/>
1547 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1548 </xs:sequence>
1549 </xs:restriction>
1550 </xs:complexContent>
1551 </xs:complexType>
1552
1553 <xs:complexType name="MobileTwoFactorContractIdentificationType">
1554 <xs:complexContent>
1555 <xs:restriction base="IdentificationType">
1556 <xs:sequence>
1557 <xs:element ref="PhysicalVerification"/>
1558 <xs:element ref="WrittenConsent"/>
1559 <xs:element ref="GoverningAgreements"/>
1560 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1561 </xs:sequence>
1562 <xs:attribute name="nym">
1563 <xs:simpleType>
1564 <xs:restriction base="xs:NMTOKEN">
1565 <xs:enumeration value="anonymity"/>
1566 <xs:enumeration value="veronymity"/>
1567 <xs:enumeration value="pseudonymity"/>
1568 </xs:restriction>
1569 </xs:simpleType>
1570 </xs:attribute>
1571 </xs:restriction>
1572 </xs:complexContent>
1573 </xs:complexType>
1574 </xs:schema>
1575
1576

```

1577 5.2.7. Password

1578 The Password class is identified when a Principal authenticates to an identity provider through the presentation of a
 1579 password over an unprotected HTTP session.

1580 5.2.7.1. Associated Liberty URI

1581 <http://www.projectliberty.org/schemas/authctx/classes/Password>

1582 5.2.7.2. Class Schema

```
1583
1584 <?xml version="1.0" encoding="UTF-8"?>
1585 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1586   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1587   xmlns="urn:liberty:ac:2003-08"
1588   version="1.2-08"
1589   finalDefault="extension">
1590 <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1591 <xs:annotation>
1592   <xs:documentation>
1593     http://www.projectliberty.org/schemas/authctx/classes/Password</xs:documentation>
1594 </xs:annotation>
1595 <xs:complexType name="PasswordAuthenticatorType">
1596   <xs:complexContent>
1597     <xs:restriction base="AuthenticatorType">
1598       <xs:choice>
1599         <xs:element ref="Password"/>
1600       </xs:choice>
1601     </xs:restriction>
1602   </xs:complexContent>
1603 </xs:complexType>
1604
1605 <xs:complexType name="PasswordPasswordType">
1606   <xs:complexContent>
1607     <xs:restriction base="PasswordType">
1608       <xs:sequence>
1609         <xs:element ref="Length" minOccurs="1"/>
1610         <xs:element ref="Generation" minOccurs="0"/>
1611         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1612       </xs:sequence>
1613     </xs:restriction>
1614   </xs:complexContent>
1615 </xs:complexType>
1616
1617 <xs:complexType name="PasswordLengthType">
1618   <xs:complexContent>
1619     <xs:restriction base="LengthType">
1620       <xs:attribute name="min" use="required">
1621         <xs:simpleType>
1622           <xs:restriction base="xs:integer">
1623             <xs:minInclusive value="3"/>
1624           </xs:restriction>
1625         </xs:simpleType>
1626       </xs:attribute>
1627       <xs:attribute name="max" type="xs:integer" use="optional"/>
1628     </xs:restriction>
1629   </xs:complexContent>
1630 </xs:complexType>
1631
1632 </xs:schema>
1633
1634
```

1635 5.2.8. PasswordProtectedTransport

1636 The PasswordProtectedTransport class is identified when a Principal authenticates to an identity provider through the
1637 presentation of a password over a protected session.

1638 5.2.8.1. Associated Liberty URI

1639 <http://www.projectliberty.org/schemas/authctx/classes/PasswordProtectedTransport>

1640 5.2.8.2. Class Schema

```
1641
1642 <?xml version="1.0" encoding="UTF-8"?>
1643 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1644   xmlns="urn:liberty:ac:2003-08"
1645   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1646   version="1.2-08"
1647   finalDefault="extension">
1648   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1649   <xs:annotation>
1650     <xs:documentation>
1651       http://www.projectliberty.org/schemas/authctx/classes/PasswordProtectedTransport</xs:documentation>
1652     </xs:annotation>
1653   <xs:complexType name="PasswordProtectedTransportAuthenticatorType">
1654     <xs:complexContent>
1655       <xs:restriction base="AuthenticatorType">
1656         <xs:choice>
1657           <xs:element ref="Password"/>
1658         </xs:choice>
1659       </xs:restriction>
1660     </xs:complexContent>
1661   </xs:complexType>
1662
1663   <xs:complexType name="PasswordProtectedTransportPasswordType">
1664     <xs:complexContent>
1665       <xs:restriction base="PasswordType">
1666         <xs:sequence>
1667           <xs:element ref="Length"/>
1668           <xs:element ref="Generation" minOccurs="0"/>
1669           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1670         </xs:sequence>
1671       </xs:restriction>
1672     </xs:complexContent>
1673   </xs:complexType>
1674
1675   <xs:complexType name="PasswordProtectedTransportLengthType">
1676     <xs:complexContent>
1677       <xs:restriction base="LengthType">
1678         <xs:attribute name="min" use="required">
1679           <xs:simpleType>
1680             <xs:restriction base="xs:integer">
1681               <xs:minInclusive value="3"/>
1682             </xs:restriction>
1683           </xs:simpleType>
1684         </xs:attribute>
1685         <xs:attribute name="max" type="xs:integer" use="optional"/>
1686       </xs:restriction>
1687     </xs:complexContent>
1688   </xs:complexType>
1689
1690   <xs:complexType name="PasswordProtectedTransportAuthenticatorTransportProtocolType">
1691     <xs:complexContent>
1692       <xs:restriction base="AuthenticatorTransportProtocolType">
1693         <xs:choice>
1694           <xs:element ref="SSL"/>
1695         </xs:choice>
1696       </xs:restriction>
1697     </xs:complexContent>
1698   </xs:complexType>
1699 </xs:schema>
1700
1701
```


1702 5.2.9. PreviousSession

1703 The PreviousSession class is identified when a Principal had authenticated to an identity provider at some point in the
1704 past using any authentication context supported by that identity provider. Consequently, a subsequent authentication
1705 event that the identity provider will assert to the service provider may be significantly separated in time from the
1706 Principals current resource access request.

1707 The context for the previously authenticated session is explicitly not included in this context class because the user
1708 has not authenticated during this session, and so the mechanism that the user employed to authenticate in a previous
1709 session should not be used as part of a decision on whether to now allow access to a resource.

1710 5.2.9.1. Associated Liberty URI

1711 <http://www.projectliberty.org/schemas/authctx/classes/PreviousSession>

1712 5.2.9.2. Class Schema

```
1713 <?xml version="1.0" encoding="UTF-8"?>
1714 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1715   xmlns="urn:liberty:ac:2003-08"
1716   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1717   version="1.2-08"
1718   finalDefault="extension">
1719   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1720   <xs:annotation>
1721     <xs:documentation>
1722       http://www.projectliberty.org/schemas/authctx/classes/PreviousSession</xs:documentation>
1723     </xs:annotation>
1724   <xs:complexType name="PreviousSessionAuthenticatorType">
1725     <xs:complexContent>
1726       <xs:restriction base="AuthenticatorType">
1727         <xs:choice>
1728           <xs:element ref="PreviousSession"/>
1729         </xs:choice>
1730       </xs:restriction>
1731     </xs:complexContent>
1732   </xs:complexType>
1733 </xs:schema>
1734
1735
1736
1737
```

1738 5.2.10. Smartcard

1739 The Smartcard class is identified when a Principal authenticates to an identity provider using a smartcard.

1740 5.2.10.1. Associated Liberty URI

1741 <http://www.projectliberty.org/schemas/authctx/classes/Smartcard>

1742 5.2.10.2. Class Schema

```
1743 <?xml version="1.0" encoding="UTF-8"?>
1744 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1745   xmlns="urn:liberty:ac:2003-08"
1746   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1747   version="1.2-08"
1748   finalDefault="extension">
1749   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1750   <xs:annotation>
1751     <xs:documentation> http://www.projectliberty.org/schemas/authctx/classes/Smartcard
1752
```

```

1753 </xs:documentation>
1754 </xs:annotation>
1755 <xs:complexType name="SmartCardPrincipalAuthenticationMechanismType">
1756 <xs:complexContent>
1757 <xs:restriction base="PrincipalAuthenticationMechanismType">
1758 <xs:choice>
1759 <xs:element ref="Smartcard"/>
1760 </xs:choice>
1761 </xs:restriction>
1762 </xs:complexContent>
1763 </xs:complexType>
1764 </xs:schema>
1765
1766

```

1767 5.2.11. SmartcardPKI

1768 The SmartcardPKI class is identified when a Principal authenticates to an identity provider through a two-factor
1769 authentication mechanism using a smartcard with enclosed private key and a PIN.

1770 5.2.11.1. Associated Liberty URI

1771 <http://www.projectliberty.org/schemas/authctx/classes/SmartcardPKI>

1772 5.2.11.2. Class Schema

```

1773
1774 <?xml version="1.0" encoding="UTF-8"?>
1775 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1776 xmlns="urn:liberty:ac:2003-08"
1777 xmlns:xs="http://www.w3.org/2001/XMLSchema"
1778 version="1.2-08"
1779 finalDefault="extension">
1780 <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1781 <xs:annotation>
1782 <xs:documentation>
1783 http://www.projectliberty.org/schemas/authctx/classes/SmartcardPKI</xs:documentation>
1784 </xs:annotation>
1785
1786 <xs:complexType name="SmartCardPKIPrincipalAuthenticationMechanismType">
1787 <xs:complexContent>
1788 <xs:restriction base="PrincipalAuthenticationMechanismType">
1789 <xs:sequence>
1790 <xs:element ref="ActivationPin"/>
1791 <xs:element ref="Smartcard"/>
1792 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1793 </xs:sequence>
1794 </xs:restriction>
1795 </xs:complexContent>
1796 </xs:complexType>
1797
1798 <xs:complexType name="SmartCardPKIAuthenticatorType">
1799 <xs:complexContent>
1800 <xs:restriction base="AuthenticatorType">
1801 <xs:choice>
1802 <xs:element ref="AsymmetricDecryption"/>
1803 <xs:element ref="AsymmetricKeyAgreement"/>
1804 <xs:element ref="DigSig"/>
1805 </xs:choice>
1806 </xs:restriction>
1807 </xs:complexContent>
1808 </xs:complexType>
1809
1810 <xs:complexType name="SmartCardPKIKeyActivationType">
1811 <xs:complexContent>

```

```

1812         <xs:restriction base="KeyActivationType">
1813             <xs:choice>
1814                 <xs:element ref="ActivationPin" />
1815             </xs:choice>
1816         </xs:restriction>
1817     </xs:complexContent>
1818 </xs:complexType>
1819
1820 <xs:complexType name="SmartcardPKIKeyStorageType">
1821     <xs:complexContent>
1822         <xs:restriction base="KeyStorageType">
1823             <xs:attribute name="medium" use="required">
1824                 <xs:simpleType>
1825                     <xs:restriction base="xs:NMTOKEN">
1826                         <xs:enumeration value="smartcard" />
1827                     </xs:restriction>
1828                 </xs:simpleType>
1829             </xs:attribute>
1830         </xs:restriction>
1831     </xs:complexContent>
1832 </xs:complexType>
1833
1834
1835 <xs:complexType name="SmartCardPKIPrivateKeyProtectionType">
1836     <xs:complexContent>
1837         <xs:restriction base="PrivateKeyProtectionType">
1838             <xs:sequence>
1839                 <xs:element ref="KeyActivation" />
1840                 <xs:element ref="KeyStorage" />
1841                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded" />
1842             </xs:sequence>
1843         </xs:restriction>
1844     </xs:complexContent>
1845 </xs:complexType>
1846
1847 </xs:schema>
1848
1849

```

1850 5.2.12. SoftwarePKI

1851 The Software-PKI class is identified when a Principal uses an X.509 certificate stored in software to authenticate to
1852 the identity provider.

1853 5.2.12.1. Associated Liberty URI

1854 <http://www.projectliberty.org/schemas/authctx/classes/SoftwarePKI>

1855 5.2.12.2. Class Schema

```

1856 <?xml version="1.0" encoding="UTF-8"?>
1857 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1858     xmlns="urn:liberty:ac:2003-08"
1859     xmlns:xs="http://www.w3.org/2001/XMLSchema"
1860     version="1.2-08"
1861     finalDefault="extension">
1862     <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd" />
1863     <xs:annotation>
1864         <xs:documentation>
1865             http://www.projectliberty.org/schemas/authctx/classes/SoftwarePKI</xs:documentation>
1866         </xs:annotation>
1867     </xs:annotation>
1868
1869     <xs:complexType name="SoftwarePKIPrincipalAuthenticationMechanismType">
1870         <xs:complexContent>

```

```
1871         <xs:restriction base="PrincipalAuthenticationMechanismType">
1872             <xs:sequence>
1873                 <xs:element ref="ActivationPin"/>
1874                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1875             </xs:sequence>
1876         </xs:restriction>
1877     </xs:complexContent>
1878 </xs:complexType>
1879
1880 <xs:complexType name="SoftwarePKIAuthenticatorType">
1881     <xs:complexContent>
1882         <xs:restriction base="AuthenticatorType">
1883             <xs:choice>
1884                 <xs:element ref="AsymmetricDecryption"/>
1885                 <xs:element ref="AsymmetricKeyAgreement"/>
1886                 <xs:element ref="DigSig"/>
1887             </xs:choice>
1888         </xs:restriction>
1889     </xs:complexContent>
1890 </xs:complexType>
1891
1892 <xs:complexType name="SoftwarePKIKeyActivationType">
1893     <xs:complexContent>
1894         <xs:restriction base="KeyActivationType">
1895             <xs:choice>
1896                 <xs:element ref="ActivationPin"/>
1897             </xs:choice>
1898         </xs:restriction>
1899     </xs:complexContent>
1900 </xs:complexType>
1901
1902 <xs:complexType name="SoftwarePKIPrivateKeyProtectionType">
1903     <xs:complexContent>
1904         <xs:restriction base="PrivateKeyProtectionType">
1905             <xs:sequence>
1906                 <xs:element ref="KeyActivation"/>
1907                 <xs:element ref="KeyStorage"/>
1908                 <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1909             </xs:sequence>
1910         </xs:restriction>
1911     </xs:complexContent>
1912 </xs:complexType>
1913
1914 <xs:complexType name="SoftwarePKIKeyStorageType">
1915     <xs:complexContent>
1916         <xs:restriction base="KeyStorageType">
1917             <xs:attribute name="medium" use="required">
1918                 <xs:simpleType>
1919                     <xs:restriction base="xs:NMTOKEN">
1920                         <xs:enumeration value="memory"/>
1921                     </xs:restriction>
1922                 </xs:simpleType>
1923             </xs:attribute>
1924         </xs:restriction>
1925     </xs:complexContent>
1926 </xs:complexType>
1927
1928 </xs:schema>
1929
1930
```

1931 **5.2.13. TimeSyncToken**

1932 The TimeSyncToken class is identified when a Principal authenticates through a time synchronization token.

1933 **5.2.13.1. Associated Liberty URI**

1934 <http://www.projectliberty.org/schemas/authctx/classes/TimeSyncToken>

1935 5.2.13.2. Class Schema

```
1936
1937 <?xml version="1.0" encoding="UTF-8"?>
1938 <xs:schema targetNamespace="urn:liberty:ac:2003-08"
1939   xmlns:xs="http://www.w3.org/2001/XMLSchema"
1940   xmlns="urn:liberty:ac:2003-08"
1941   finalDefault="extension">
1942   <xs:include schemaLocation="lib-arch-authentication-context-v1.2-08.xsd"/>
1943   <xs:annotation>
1944     <xs:documentation> http://www.projectliberty.org/schemas/authctx/classes/TimeSyncToken</xs:
1945 documentation>
1946   </xs:annotation>
1947   <xs:complexType name="TimeSyncTokenPrincipalAuthenticationMechanismType">
1948     <xs:complexContent>
1949       <xs:restriction base="PrincipalAuthenticationMechanismType">
1950         <xs:choice>
1951           <xs:element ref="Token"/>
1952         </xs:choice>
1953       </xs:restriction>
1954     </xs:complexContent>
1955   </xs:complexType>
1956   <xs:complexType name="TimeSyncTokenTokenType">
1957     <xs:complexContent>
1958       <xs:restriction base="TokenType">
1959         <xs:sequence>
1960           <xs:element ref="TimeSyncToken"/>
1961           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
1962         </xs:sequence>
1963       </xs:restriction>
1964     </xs:complexContent>
1965   </xs:complexType>
1966   <xs:complexType name="TimeSyncTokenTimeSyncTokenType">
1967     <xs:complexContent>
1968       <xs:restriction base="TimeSyncTokenType">
1969         <xs:attribute name="DeviceType" use="required">
1970           <xs:simpleType>
1971             <xs:restriction base="xs:NMTOKEN">
1972               <xs:enumeration value="hardware"/>
1973             </xs:restriction>
1974           </xs:simpleType>
1975         </xs:attribute>
1976         <xs:attribute name="SeedLength" use="required">
1977           <xs:simpleType>
1978             <xs:restriction base="xs:integer">
1979               <xs:enumeration value="64"/>
1980             </xs:restriction>
1981           </xs:simpleType>
1982         </xs:attribute>
1983         <xs:attribute name="DeviceInHand" use="required">
1984           <xs:simpleType>
1985             <xs:restriction base="xs:NMTOKEN">
1986               <xs:enumeration value="true"/>
1987             </xs:restriction>
1988           </xs:simpleType>
1989         </xs:attribute>
1990       </xs:restriction>
1991     </xs:complexContent>
1992   </xs:complexType>
1993 </xs:schema>
1994
1995
```

1996 5.3. Authentication Context Classes Extensibility

1997 As did the core Authentication Context Statement schema, the separate Authentication Context Classes schemas allow
1998 the <Extension> element in certain locations of the tree structure. In general, where the <Extension> element occurred
1999 as a child of a <Choice> element, this option was removed in creating the appropriate class schema definition as an
2000 extension of the base type. When the <Extension> element occurred as an optional child of a <Sequence> element,
2001 the <Extension> element was allowed to remain in addition to any required elements.

2002 Consequently, authentication context statements can include the <Extension> element (with additional elements in
2003 different namespaces) and still conform to authentication context class schemas (if they meet the other requirements
2004 of the schema of course)

2005 The Authentication Context Class schemas extend (as restrictions) appropriate type definitions in the core Authentica-
2006 tion Context Statement schema. As an extension point, the Authentication Context Classes schemas themselves can be
2007 extended - their type definitions serving as base types in some other schema (potentially defined by some community
2008 wishing a more tightly defined authentication context class). To prevent logical inconsistencies, any such extensions
2009 can only further constrain the type definitions of the core Authentication Context Statement schema. To enforce this
2010 constraint, the Authentication Context Class schemas are defined with the finalDefault="extension" attribute on the
2011 <schema> element to prevent this type of extension derivation.

2012 **5.4. Authentication Context Classes Processing Rules**

2013 The processing rules for both Service and Identity Provider for Authentication Context Classes are listed in [[LibertyProtSchema](#)].
2014

2015 **References**

2016 **References**

- 2017 [LibertyProtSchema] Cantor, Scott, Kemp, John, eds. "Liberty ID-FF Protocols and Schema Specification," Version
2018 1.2-errata-v2.0, Liberty Alliance Project (12 September 2004). <http://www.projectliberty.org/specs>
- 2019 [RFC2119] Bradner, S., eds. "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, The Internet
2020 Engineering Task Force (March 1997). <http://www.ietf.org/rfc/rfc2119.txt> [March 1997].
- 2021 [Schema1] Thompson, Henry S., Beech, David, Maloney, Murray, Mendelsohn, Noah, eds. (May
2022 2002). "XML Schema Part 1: Structures," Recommendation, World Wide Web Consortium
2023 <http://www.w3.org/TR/xmlschema-1/>