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

Committee Draft 01, 18 August 2004

Document identifier:
sstc-saml-authn-context-2.0-cd-01

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

Editors:
John Kemp, Nokia
Rob Philpott, RSA Security
Eve Maler, Sun Microsystems

SAML V2.0 Contributors:
Conor P. Cahill, AOL
Hal Lockhart, BEA Systems
Michael Beach, Boeing
Rick Randall, Booze, Allen, Hamilton
Tim Alsop, Cybersafe
Nick Ragouzis, Enosis
John Hughes, Entegrity Solutions
Paul Madsen, Entrust
Irving Reid, Hewlett-Packard
Paula Austel, IBM
Maryann Hondo, IBM
Michael McIntosh, IBM
Tony Nadalin, IBM
Scott Cantor, Internet2
RL 'Bob' Morgan, Internet2
Rebekah Metz, NASA
Prateek Mishra, Netegrity
Peter C Davis, Neustar
Frederick Hirsch, Nokia
John Kemp, Nokia
Charles Knouse, Oblix
Steve Anderson, OpenNetwork
John Linn, RSA Security
Rob Philpott, RSA Security
Jahan Moreh, Sigaba
Anne Anderson, Sun Microsystems
Jeff Hodges, Sun Microsystems
Eve Maler, Sun Microsystems
Ron Monzillo, Sun Microsystems
Greg Whitehead, Trustgenix

Abstract:

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

Status:

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

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

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

Table of Contents

1 Introduction

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

1.1 Authentication Context Concepts

If a service provider is to rely on the authentication of a Principal by an authentication authority (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 declarations - 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 declarations will fall, thereby simplifying their interpretation.

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

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

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

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

1.2 Notation and Terminology

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

```
Listings of XML schemas appear like this.
```

```
Example code listings appear like this.
```

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

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

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

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

2 Authentication Context Declaration

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

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

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

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

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

2.1 Data Model

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

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

2.2 Extensibility

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

2.3 Processing Rules

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

2.4 Schema

This section lists the complete Authentication Context XML Schema.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac">

  <xs:element name="AuthenticationContextDeclaration"
    type="AuthnContextDeclarationBaseType">
    <xs:annotation>
      <xs:documentation>
        A particular assertion on an identity
        provider's part with respect to the authentication
        context associated with an authentication assertion.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Identification" type="IdentificationType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that describe the
        processes and mechanisms
        the Authentication Authority uses to initially create
        an association between a Principal
        and the identity (or name) by which the Principal will
        be known
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PhysicalVerification">
    <xs:annotation>
      <xs:documentation>
        This element indicates that identification has been
        performed in a physical
        face-to-face meeting with the principal and not in an
        online manner.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:attribute name="credentialLevel">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
```

```
            <xs:enumeration value="primary"/>
            <xs:enumeration value="secondary"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>

  <xs:element name="WrittenConsent">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="TechnicalProtection"
    type="TechnicalProtectionBaseType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characterstics that describe how the
        'secret' (the knowledge or possession
        of which allows the Principal to authenticate to the
        Authentication Authority) is kept secure
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SecretKeyProtection"
    type="SecretKeyProtectionType">
    <xs:annotation>
      <xs:documentation>
        This element indicates the types and strengths of
        facilities
        of a UA used to protect a shared secret key from
        unauthorized access and/or use.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PrivateKeyProtection"
    type="PrivateKeyProtectionType">
    <xs:annotation>
      <xs:documentation>
        This element indicates the types and strengths of
        facilities
        of a UA used to protect a private key from
        unauthorized access and/or use.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="KeyActivation" type="KeyActivationType">
    <xs:annotation>
      <xs:documentation>The actions that must be performed
        before the private key can be used. </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="KeySharing" type="KeySharingType">
```

```
    <xs:annotation>
      <xs:documentation>Whether or not the private key is shared
        with the certificate authority.</xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="KeyStorage" type="KeyStorageType">
    <xs:annotation>
      <xs:documentation>
        In which medium is the key stored.
        memory - the key is stored in memory.
        smartcard - the key is stored in a smartcard.
        token - the key is stored in a hardware token.
        MobileDevice - the key is stored in a mobile device.
        MobileAuthCard - the key is stored in a mobile
        authentication card.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SubscriberLineNumber">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="UserSuffix">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="Password" type="PasswordType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that a password (or passphrase)
        has been used to
        authenticate the Principal to a remote system.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ActivationPin" type="ActivationPinType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that a Pin (Personal
        Identification Number) has been used to authenticate the
Principal to
        some local system in order to activate a key.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Token" type="TokenType">
    <xs:annotation>
```

```
      <xs:documentation>
        This element indicates that a hardware or software
        token is used
        as a method of identifying the Principal.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="TimeSyncToken" type="TimeSyncTokenType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that a time synchronization
        token is used to identify the Principal. hardware -
        the time synchonization
        token has been implemented in hardware. software - the
        time synchronization
        token has been implemented in software. SeedLength -
        the length, in bits, of the
        random seed used in the time synchronization token.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Smartcard">
    <xs:annotation>
      <xs:documentation>
        This element indicates that a smartcard is used to
        identity the Principal.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="Length" type="LengthType">
    <xs:annotation>
      <xs:documentation>
        This element indicates the minimum and/or maximum
        ASCII length of the password which is enforced (by the UA
or the
        IdP). In other words, this is the minimum and/or maximum
number of
        ASCII characters required to represent a valid password.
        min - the minimum number of ASCII characters required
        in a valid password, as enforced by the UA or the IdP.
        max - the maximum number of ASCII characters required
        in a valid password, as enforced by the UA or the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ActivationLimit" type="ActivationLimitType">
    <xs:annotation>
      <xs:documentation>
        This element indicates the length of time for which an
        PIN-based authentication is valid.
      </xs:documentation>
```

```
    </xs:annotation>
  </xs:element>

  <xs:element name="Generation">
    <xs:annotation>
      <xs:documentation>
        Indicates whether the password was chosen by the
        Principal or auto-supplied by the Authentication
Authority.
        principalchosen - the Principal is allowed to choose
        the value of the password. This is true even if
        the initial password is chosen at random by the UA or
        the IdP and the Principal is then free to change
        the password.
        automatic - the password is chosen by the UA or the
        IdP to be cryptographically strong in some sense,
        or to satisfy certain password rules, and that the
        Principal is not free to change it or to choose a new
password.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType>
      <xs:attribute name="mechanism" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="principalchosen"/>
            <xs:enumeration value="automatic"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>

  <xs:element name="AuthenticationMethod"
    type="AuthnMethodBaseType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that define the
        mechanisms by which the Principal authenticates to the
Authentication
        Authority.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PrincipalAuthenticationMechanism"
    type="PrincipalAuthenticationMechanismType">
    <xs:annotation>
      <xs:documentation>
        The method that a Principal employs to perform
        authentication to local system components.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Authenticator" type="AuthenticatorBaseType">
    <xs:annotation>
      <xs:documentation>
        The method applied to validate a principal's
        authentication across a network
```

```
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PreviousSession">
    <xs:annotation>
      <xs:documentation>
        Indicates that the Principal has been strongly
        authenticated in a previous session during which the IdP
has set a
        cookie in the UA. During the present session the
Principal has only
        been authenticated by the UA returning the cookie to the
IdP.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="ResumeSession">
    <xs:annotation>
      <xs:documentation>
        Rather like PreviousSession but using stronger
        security. A secret that was established in a previous
session with
        the Authentication Authority has been cached by the local
system and
        is now re-used (e.g. a Master Secret is used to derive
new session
        keys in TLS, SSL, WTLS).
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="ZeroKnowledge">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a zero knowledge technique as specified
in ISO/IEC
        9798-5.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
```

```
  <xs:element name="SharedSecretChallengeResponse"
type="SharedSecretChallengeResponseType"/>

  <xs:complexType name="SharedSecretChallengeResponseType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a challenge-response protocol utilizing
shared secret
        keys and symmetric cryptography.
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="method" type="xs:anyURI" use="optional"/>
  </xs:complexType>

  <xs:element name="DigSig" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a mechanism which involves the Principal
computing a
        digital signature over at least challenge data provided
by the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AsymmetricDecryption" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        The local system has a private key but it is used
        in decryption mode, rather than signature mode. For
example, the
        Authentication Authority generates a secret and encrypts
it using the
        local system's public key: the local system then proves
it has
        decrypted the secret.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AsymmetricKeyAgreement" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        The local system has a private key and uses it for
        shared secret key agreement with the Authentication
Authority (e.g.
        via Diffie Helman).
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:complexType name="PublicKeyType">
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0"
```

```
        maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="keyValidation" use="optional"/>
  </xs:complexType>

  <xs:element name="IPAddress">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated through connection from a particular IP
address.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="SharedSecretDynamicPlaintext"
type="SharedSecretDynamicPlaintextType"/>

  <xs:annotation>
    <xs:documentation>
      The local system and Authentication Authority
      share a secret key. The local system uses this to encrypt a
      randomised string to pass to the Authentication Authority.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="SharedSecretDynamicPlaintextType">
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="AuthenticatorTransportProtocol"
    type="AuthenticatorTransportProtocolType">
    <xs:annotation>
      <xs:documentation>
        The protocol across which Authenticator information is
        transferred to an Authentication Authority verifier.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="HTTP">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using bare HTTP utilizing no additional
security
        protocols.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
```

```
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="IPSec">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using a transport mechanism protected by an
IPSEC session.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="WTLS">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using a transport mechanism protected by a
WTLS session.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="MobileNetworkNoEncryption">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted solely across a mobile network using no
additional
        security mechanism.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="MobileNetworkRadioEncryption">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="MobileNetworkEndToEndEncryption">
    <xs:complexType>
```

```
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="SSL">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using a transport mechnanism protected by an
SSL or TLS
        session.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="PSTN">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="ISDN">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="ADSL">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="OperationalProtection"
    type="OperationalProtectionType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that describe
        procedural security controls employed by the
Authentication Authority.
      </xs:documentation>
    </xs:annotation>
  </xs:element>
```

```
  <xs:element name="SecurityAudit" type="SecurityAuditType"/>

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

  <xs:element name="DeactivationCallCenter">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Extension" minOccurs="0"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="GoverningAgreements"
    type="GoverningAgreementsType">
    <xs:annotation>
      <xs:documentation>
        Provides a mechanism for linking to external (likely
        human readable) documents in which additional business
agreements,
        (e.g. liability constraints, obligations, etc) can be
placed.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="GoverningAgreementRef"
    type="GoverningAgreementRefType"/>

  <xs:complexType name="IdentificationType">
    <xs:sequence>
      <xs:element ref="PhysicalVerification" minOccurs="0"/>
      <xs:element ref="WrittenConsent" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="nym">
      <xs:annotation>
        <xs:documentation>
          This attribute indicates whether or not the
          Identification mechanisms allow the actions of the
Principal to be
          linked to an actual end user.
        </xs:documentation>
      </xs:annotation>
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="anonymity"/>
          <xs:enumeration value="verinymity"/>
          <xs:enumeration value="pseudonymity"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
```

```
  </xs:complexType>

  <xs:complexType name="GoverningAgreementsType">
    <xs:sequence>
      <xs:element ref="GoverningAgreementRef"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="GoverningAgreementRefType">
    <xs:attribute name="governingAgreementRef" type="xs:anyURI"
      use="required"/>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:choice>
      <xs:element ref="HTTP"/>
      <xs:element ref="SSL"/>
      <xs:element ref="MobileNetworkNoEncryption"/>
      <xs:element ref="MobileNetworkRadioEncryption"/>
      <xs:element ref="MobileNetworkEndToEndEncryption"/>
      <xs:element ref="WTLS"/>
      <xs:element ref="IPSec"/>
      <xs:element ref="PSTN"/>
      <xs:element ref="ISDN"/>
      <xs:element ref="ADSL"/>
      <xs:element ref="Extension" maxOccurs="unbounded"/>
    </xs:choice>
  </xs:complexType>

  <xs:complexType name="PrincipalAuthenticationMechanismType">
    <xs:sequence>
      <xs:choice>
        <xs:element ref="Password"/>
        <xs:element ref="Token"/>
        <xs:element ref="Smartcard"/>
        <xs:element ref="ActivationPin"/>
        <xs:element ref="Extension" maxOccurs="unbounded"/>
      </xs:choice>
    </xs:sequence>
    <xs:attribute name="preauth" type="xs:integer"
use="optional"/>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:sequence>
      <xs:element ref="PrincipalAuthenticationMechanism"
        minOccurs="0"/>
      <xs:element ref="Authenticator" minOccurs="0"/>
      <xs:element ref="AuthenticatorTransportProtocol"
        minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:sequence>
      <xs:element ref="Identification" minOccurs="0"/>
      <xs:element ref="TechnicalProtection" minOccurs="0"/>
      <xs:element ref="OperationalProtection" minOccurs="0"/>
```

```
      <xs:element ref="AuthenticationMethod" minOccurs="0"/>
      <xs:element ref="GoverningAgreements" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="ID" type="xs:ID"/>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:choice>
      <xs:element ref="PrivateKeyProtection" minOccurs="0"/>
      <xs:element ref="SecretKeyProtection" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:choice>
  </xs:complexType>

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

  <xs:complexType name="AuthenticatorBaseType">
    <xs:choice>
      <xs:element ref="PreviousSession"/>
      <xs:element ref="ResumeSession"/>
      <xs:element ref="DigSig"/>
      <xs:element ref="Password"/>
      <xs:element ref="ZeroKnowledge"/>
      <xs:element ref="SharedSecretChallengeResponse"/>
      <xs:element ref="SharedSecretDynamicPlaintext"/>
      <xs:element ref="IPAddress"/>
      <xs:element ref="AsymmetricDecryption"/>
      <xs:element ref="AsymmetricKeyAgreement"/>
      <xs:element ref="SubscriberLineNumber"/>
      <xs:element ref="UserSuffix"/>
      <xs:element ref="Extension" maxOccurs="unbounded"/>
    </xs:choice>
  </xs:complexType>

  <xs:complexType name="KeyActivationType">
    <xs:choice>
      <xs:element ref="ActivationPin"/>
      <xs:element ref="Extension" maxOccurs="unbounded"/>
    </xs:choice>
  </xs:complexType>

  <xs:complexType name="KeySharingType">
    <xs:attribute name="sharing" type="xs:boolean"
      use="required"/>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:sequence>
      <xs:element ref="KeyActivation" minOccurs="0"/>
      <xs:element ref="KeyStorage" minOccurs="0"/>
      <xs:element ref="KeySharing" minOccurs="0"/>
```

```
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="PasswordType">
    <xs:sequence>
      <xs:element ref="Length" minOccurs="0"/>
      <xs:element ref="Alphabet" minOccurs="0"/>
      <xs:element ref="Generation" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="ExternalVerification" type="xs:anyURI"
use="optional"/>
  </xs:complexType>

  <xs:element name="RestrictedPassword"
type="RestrictedPasswordType"/>

  <xs:complexType name="RestrictedPasswordType">
    <xs:complexContent>
      <xs:restriction base="PasswordType">
        <xs:sequence>
          <xs:element ref="RestrictedLength" minOccurs="1"/>
          <xs:element ref="Generation" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ExternalVerification"
type="xs:anyURI" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="RestrictedLength"
type="RestrictedLengthType"/>

  <xs:complexType name="RestrictedLengthType">
    <xs:complexContent>
      <xs:restriction base="LengthType">
        <xs:attribute name="min" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="3"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="max" type="xs:integer"
use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="ActivationPinType">
    <xs:sequence>
      <xs:element ref="Length" minOccurs="0"/>
      <xs:element ref="Alphabet" minOccurs="0"/>
      <xs:element ref="Generation" minOccurs="0"/>
      <xs:element ref="ActivationLimit" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0"
```

```
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:element name="Alphabet" type="AlphabetType"/>
  <xs:complexType name="AlphabetType">
    <xs:attribute name="requiredChars" type="xs:string"
      use="required"/>
    <xs:attribute name="excludedChars" type="xs:string"
      use="optional"/>
    <xs:attribute name="case" type="xs:string" use="optional"/>
  </xs:complexType>
  <xs:complexType name="TokenType">
    <xs:sequence>
      <xs:element ref="TimeSyncToken"/>
      <xs:element ref="Extension" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="TimeSyncTokenType">
    <xs:attribute name="DeviceType" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="hardware"/>
          <xs:enumeration value="software"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="SeedLength" type="xs:integer"
      use="required"/>
    <xs:attribute name="DeviceInHand" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="true"/>
          <xs:enumeration value="false"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
  </xs:complexType>
  <xs:complexType name="ActivationLimitType">
    <xs:choice>
      <xs:element ref="ActivationLimitDuration"/>
      <xs:element ref="ActivationLimitUsages"/>
      <xs:element ref="ActivationLimitSession"/>
    </xs:choice>
  </xs:complexType>
  <xs:element name="ActivationLimitDuration"
    type="ActivationLimitDurationType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Key Activation Limit is
        defined as a specific duration of time.
      </xs:documentation>
    </xs:annotation>
  </xs:element>
  <xs:element name="ActivationLimitUsages"
    type="ActivationLimitUsagesType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Key Activation Limit is
        defined as a number of usages.
      </xs:documentation>
```

```
    </xs:annotation>
  </xs:element>
  <xs:element name="ActivationLimitSession"
    type="ActivationLimitSessionType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Key Activation Limit is
        the session.
      </xs:documentation>
    </xs:annotation>
  </xs:element>
  <xs:complexType name="ActivationLimitDurationType">
    <xs:attribute name="duration" type="xs:duration"
      use="required"/>
  </xs:complexType>
  <xs:complexType name="ActivationLimitUsagesType">
    <xs:attribute name="number" type="xs:integer"
      use="required"/>
  </xs:complexType>
  <xs:complexType name="ActivationLimitSessionType"/>
  <xs:complexType name="LengthType">
    <xs:attribute name="min" type="xs:integer" use="required"/>
    <xs:attribute name="max" type="xs:integer" use="optional"/>
  </xs:complexType>

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

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

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

  <xs:element name="Extension" type="ExtensionType"/>

  <xs:complexType name="ExtensionType">
    <xs:sequence>
      <xs:any namespace="##other" processContents="lax"
maxOccurs="unbounded"/>
```

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

</xs:schema>
```

3 Authentication Context Classes

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

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

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

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

3.1 Advantages of Authentication Context Classes

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

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

3.2 Processing Rules

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

3.3 Extensibility

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

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

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

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

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

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

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

3.4 Schemas

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

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

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

3.4.1 Internet Protocol

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="InternetProtocolType"/>

  <xs:complexType name="InternetProtocolType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:IPAddress"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

```

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

3.4.2 InternetProtocolPassword

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolP
assword"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
```

```
  </xs:complexType>

  <xs:element name="Authenticator" type="InternetProtocolType"/>

  <xs:complexType name="InternetProtocolType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="ac:IPAddress"/>
          <xs:element ref="ac:Password"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.3 Kerberos

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

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

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

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

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

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

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
```

```
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism" type="PasswordAuthnMechanismType"/>

  <xs:complexType name="PasswordAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="ac:RestrictedPassword"/>
          </xs:choice>
        </xs:sequence>
        <xs:attribute name="preauth" type="xs:integer" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="SharedSecretType"/>

  <xs:complexType name="SharedSecretType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="SharedSecretChallengeResponse"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="SharedSecretChallengeResponse"
type="ChallengeResponseType"/>

  <xs:complexType name="ChallengeResponseType">
    <xs:complexContent>
      <xs:restriction base="ac:SharedSecretChallengeResponseType">
        <xs:attribute name="method"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

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

```
<?xml version="1.0" encoding="UTF-8"?>
    <AuthnContextDeclaration
        xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos">

        <AuthnMethod>
            <PasswordAuthnMechanism preauth="0">
                <ac:Password/>
            <PasswordAuthnMechanism>
            <Authenticator>
                <SharedSecretChallengeResponse
method="urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos"/>
            </Authenticator>
        </AuthnMethod>

    </AuthnContextDeclaration>
```

3.4.4 MobileOneFactorUnregistered

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUn
registered"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregister
ed"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
```

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

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

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

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

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

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

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

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

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

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

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

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

  <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>

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

  <xs:element name="KeyStorage" type="KeyStorageType"/>

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

  <xs:element name="SecurityAudit" type="SecurityAuditType"/>

  <xs:complexType name="SecurityAuditType">
    <xs:complexContent>
```

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

  <xs:element name="Identification" type="IdentificationType"/>

  <xs:complexType name="IdentificationType">
    <xs:complexContent>
      <xs:restriction base="ac:IdentificationType">
        <xs:attribute name="nym">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="anonymity"/>
              <xs:enumeration value="pseudonymity"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.5 MobileTwoFactorUnregistered

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUn
registered"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregister
ed"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
```

```
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:DigSig"/>
          <xs:element ref="ac:ZeroKnowledge"/>
          <xs:element ref="ac:SharedSecretChallengeResponse"/>
          <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
          <xs:element ref="ac:AsymmetricDecryption"/>
          <xs:element ref="ac:AsymmetricKeyAgreement"/>
          <xs:sequence>
            <xs:element ref="ac:Password" minOccurs="1"/>
            <xs:choice>
              <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
              <xs:element ref="ac:SharedSecretChallengeResponse"/>
            </xs:choice>
            <xs:element ref="ac:Extension" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

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

```
          <xs:element ref="ac:MobileNetworkEndToEndEncryption"/>
          <xs:element ref="ac:WTLS"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

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

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

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

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

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

  <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>

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

```

```
  <xs:element name="KeyActivation" type="KeyActivationType"/>

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

  <xs:element name="KeyStorage" type="KeyStorageType"/>

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

  <xs:element name="SecurityAudit" type="SecurityAuditType"/>

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

  <xs:element name="Identification" type="IdentificationType"/>

  <xs:complexType name="IdentificationType">
    <xs:complexContent>
      <xs:restriction base="ac:IdentificationType">
        <xs:attribute name="nym">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="anonymity"/>
              <xs:enumeration value="pseudonymity"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.6 MobileOneFactorContract

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorCo
ntract"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
  <xs:element name="Authenticator" type="AuthenticatorType"/>

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

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

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

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

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

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

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

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

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

  <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>

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

  <xs:element name="KeyStorage" type="KeyStorageType"/>

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

  <xs:element name="SecurityAudit" type="SecurityAuditType"/>

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

  <xs:element name="Identification" type="IdentificationType"/>

  <xs:complexType name="IdentificationType">
    <xs:complexContent>
      <xs:restriction base="ac:IdentificationType">
        <xs:sequence>
          <xs:element ref="ac:PhysicalVerification"/>
          <xs:element ref="ac:WrittenConsent"/>
          <xs:element ref="ac:GoverningAgreements"/>
```

```
          <xs:element ref="ac:Extension" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="nym">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="anonymity"/>
              <xs:enumeration value="verinymity"/>
              <xs:enumeration value="pseudonymity"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.7 MobileTwoFactorContract

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorCo
ntract"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:DigSig"/>
          <xs:element ref="ac:ZeroKnowledge"/>
          <xs:element ref="ac:SharedSecretChallengeResponse"/>
          <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
          <xs:element ref="ac:AsymmetricDecryption"/>
          <xs:element ref="ac:AsymmetricKeyAgreement"/>
          <xs:sequence>
            <xs:element ref="ac:Password" minOccurs="1"/>
            <xs:choice>
              <xs:element ref="ac:SharedSecretDynamicPlaintext"/>
              <xs:element ref="ac:SharedSecretChallengeResponse"/>
            </xs:choice>
            <xs:element ref="ac:Extension" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

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

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

  <xs:complexType name="OperationalProtectionType">
    <xs:complexContent>
      <xs:restriction base="OperationalProtectionType">
```

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

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

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

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

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

  <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType"/>

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

  <xs:element name="KeyActivation" type="KeyActivationType"/>

  <xs:complexType name="KeyActivationType">
    <xs:complexContent>
      <xs:restriction base="ac:KeyActivationType">
        <xs:sequence>
          <xs:element ref="ac:ActivationPin"/>
          <xs:element ref="ac:Extension" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
  <xs:element name="KeyStorage" type="KeyStorageType"/>

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

  <xs:element name="SecurityAudit" type="SecurityAuditType"/>

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

  <xs:element name="Identification" type="IdentificationType"/>

  <xs:complexType name="IdentificationType">
    <xs:complexContent>
      <xs:restriction base="ac:IdentificationType">
        <xs:sequence>
          <xs:element ref="ac:PhysicalVerification"/>
          <xs:element ref="ac:WrittenConsent"/>
          <xs:element ref="ac:GoverningAgreements"/>
          <xs:element ref="ac:Extension" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="nym">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="anonymity"/>
              <xs:enumeration value="verinymity"/>
              <xs:enumeration value="pseudonymity"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.8 Password

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:Password
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:RestrictedPassword"/>
        </xs:choice>
      </xs:restriction>
```

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

</xs:schema>
```

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

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

    <AuthenticationContextDeclaration
        xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password">

        <AuthnMethod>
            <Authenticator>
                <ac:RestrictedPassword>
                    <ac:RestrictedLength min="4"/>
                </ac:RestrictedPassword>
            </Authenticator>
        </AuthnMethod>

    </AuthenticationContextDeclaration>
```

3.4.9 PasswordProtectedTransport

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected
Transport"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspor
t"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
```

```
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:RestrictedPassword"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

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

</xs:schema>
```

3.4.10 PreviousSession

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

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="PreviousSessionType"/>

  <xs:complexType name="PreviousSessionType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:PreviousSession"/>
```

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

</xs:schema>
```

3.4.11 Public Key – X.509

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:X509
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection"
minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority"
minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
```

```
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism"
type="PasswordAuthnMechanismType"/>

  <xs:complexType name="PasswordAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction
base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="ac:RestrictedPassword"/>
          </xs:choice>
        </xs:sequence>
        <xs:attribute name="preauth" type="xs:integer"
use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="DigSig"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="DigSig" type="DigSigType"/>

  <xs:complexType name="DigSigType">
    <xs:complexContent>
      <xs:restriction base="ac:PublicKeyType">
        <xs:attribute name="keyValidation"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.12 Public Key – PGP

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection"
minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority"
minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism"
type="PasswordAuthnMechanismType"/>

```

```
  <xs:complexType name="PasswordAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction
base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="ac:RestrictedPassword"/>
          </xs:choice>
        </xs:sequence>
        <xs:attribute name="preauth" type="xs:integer"
use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="DigSig"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="DigSig" type="DigSigType"/>

  <xs:complexType name="DigSigType">
    <xs:complexContent>
      <xs:restriction base="ac:PublicKeyType">
        <xs:attribute name="keyValidation"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.13 Public Key – SPKI

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>
```

```
  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection"
minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority"
minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism"
type="PasswordAuthnMechanismType"/>

  <xs:complexType name="PasswordAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction
base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="ac:RestrictedPassword"/>
          </xs:choice>
        </xs:sequence>
        <xs:attribute name="preauth" type="xs:integer"
use="optional"/>
      </xs:restriction>
    </xs:complexContent>
```

```
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="DigSig"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="DigSig" type="DigSigType"/>

  <xs:complexType name="DigSigType">
    <xs:complexContent>
      <xs:restriction base="ac:PublicKeyType">
        <xs:attribute name="keyValidation"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.14 Public Key - XML Digital Signature

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
```

```
          <xs:element ref="ac:OperationalProtection"
minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority"
minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism"
type="PasswordAuthnMechanismType"/>

  <xs:complexType name="PasswordAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction
base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="ac:RestrictedPassword"/>
          </xs:choice>
        </xs:sequence>
        <xs:attribute name="preauth" type="xs:integer"
use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="DigSig"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
  <xs:element name="DigSig" type="DigSigType"/>

  <xs:complexType name="DigSigType">
    <xs:complexContent>
      <xs:restriction base="ac:PublicKeyType">
        <xs:attribute name="keyValidation"
fixed="urn:ietf:rfc:3075"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.15 Smartcard

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

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

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

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

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

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
```

```
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="ac:Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>

  <xs:complexType name="SmartcardAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="ac:Smartcard"/>
          </xs:choice>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.16 SmartcardPKI

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

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

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

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

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac" schemaLocation="sstc-saml-
schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
```

```
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

  <xs:complexType name="TechnicalProtectionType">
    <xs:complexContent>
      <xs:restriction base="ac:TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="ac:SecretKeyProtection" minOccurs="0"/>
            <xs:element ref="ac:Extension" minOccurs="0"
              maxOccurs="unbounded"/>
          </xs:choice>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>

  <xs:complexType name="SmartcardAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
            <xs:element ref="ac:ActivationPin"/>
            <xs:element ref="ac:Smartcard"/>
            <xs:element ref="ac:Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="SmartCardPKIAuthenticatorType"/>

  <xs:complexType name="SmartCardPKIAuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:AsymmetricDecryption"/>
          <xs:element ref="ac:AsymmetricKeyAgreement"/>
          <xs:element ref="ac:DigSig"/>
        </xs:choice>
```

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

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

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

  <xs:element name="KeyActivation" type="KeyActivationType"/>

  <xs:complexType name="KeyActivationType">
    <xs:complexContent>
      <xs:restriction base="ac:KeyActivationType">
        <xs:choice>
          <xs:element ref="ac:ActivationPin"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="KeyStorage" type="KeyStorageType"/>

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

</xs:schema>
```

3.4.17 SoftwarePKI

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
  finalDefault="extension">
```

```
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

  <xs:complexType name="TechnicalProtectionType">
    <xs:complexContent>
      <xs:restriction base="ac:TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="ac:SecretKeyProtection" minOccurs="0"/>
            <xs:element ref="ac:Extension" minOccurs="0"
              maxOccurs="unbounded"/>
          </xs:choice>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism" type="SmartcardAuthnMechanismType"/>

  <xs:complexType name="SmartcardAuthnMechanismType">
    <xs:complexContent>
```

```
      <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
            <xs:element ref="ac:ActivationPin"/>
            <xs:element ref="ac:Extension" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="SmartCardPKIAuthenticatorType"/>

  <xs:complexType name="SmartCardPKIAuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:AsymmetricDecryption"/>
          <xs:element ref="ac:AsymmetricKeyAgreement"/>
          <xs:element ref="ac:DigSig"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

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

  <xs:element name="KeyActivation" type="KeyActivationType"/>

  <xs:complexType name="KeyActivationType">
    <xs:complexContent>
      <xs:restriction base="ac:KeyActivationType">
        <xs:choice>
          <xs:element ref="ac:ActivationPin"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="KeyStorage" type="KeyStorageType"/>

  <xs:complexType name="KeyStorageType">
    <xs:complexContent>
      <xs:restriction base="ac:KeyStorageType">
        <xs:attribute name="medium" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="memory"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

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

3.4.18 Telephony

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="ac:SubscriberLineNumber"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

  <xs:complexType name="TransportType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorTransportProtocolType">
        <xs:choice>
          <xs:element ref="ac:PSTN"/>
          <xs:element ref="ac:ISDN"/>
          <xs:element ref="ac:ADSL"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.19 Telephony ("Nomadic")

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
```

```
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="ac:SubscriberLineNumber"/>
          <xs:element ref="ac:UserSuffix"/>
          <xs:element ref="ac:Password"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

  <xs:complexType name="TransportType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorTransportProtocolType">
        <xs:choice>
          <xs:element ref="ac:PSTN"/>
          <xs:element ref="ac:ISDN"/>
          <xs:element ref="ac:ADSL"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.20 Telephony (Personalized)

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelep
hony"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="ac:SubscriberLineNumber"/>
          <xs:element ref="ac:UserSuffix"/>
        </xs:sequence>
```

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

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

  <xs:complexType name="TransportType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorTransportProtocolType">
        <xs:choice>
          <xs:element ref="ac:PSTN"/>
          <xs:element ref="ac:ISDN"/>
          <xs:element ref="ac:ADSL"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.21 Telephony (Authenticated)

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTele
phony"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
```

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

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="ac:PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="ac:SubscriberLineNumber"/>
          <xs:element ref="ac:UserSuffix"/>
          <xs:element ref="ac:Password"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

  <xs:complexType name="TransportType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorTransportProtocolType">
        <xs:choice>
          <xs:element ref="ac:PSTN"/>
          <xs:element ref="ac:ISDN"/>
          <xs:element ref="ac:ADSL"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.22 Secure Remote Password

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRem
otePassword"
```

```
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassw
ord"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection"
minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority"
minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="PrincipalAuthenticationMechanism"
type="PasswordAuthnMechanismType"/>

  <xs:complexType name="PasswordAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction
base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
```

```
          <xs:choice>
            <xs:element ref="ac:RestrictedPassword"/>
          </xs:choice>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="SharedSecretType"/>

  <xs:complexType name="SharedSecretType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
        <xs:choice>
          <xs:element ref="SharedSecretChallengeResponse"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="SharedSecretChallengeResponse"
type="ChallengeResponseType"/>

  <xs:complexType name="ChallengeResponseType">
    <xs:complexContent>
      <xs:restriction base="ac:SharedSecretChallengeResponseType">
        <xs:attribute name="method" fixed="urn:ietf:rfc:2945"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.23 SSL/TLS Certificate-Based Client Authentication

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
    </xs:documentation>
  </xs:annotation>
```

```
  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection"
minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority"
minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="AuthnMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMechanism"
type="PasswordAuthnMechanismType"/>

  <xs:complexType name="PasswordAuthnMechanismType">
    <xs:complexContent>
      <xs:restriction
base="ac:PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="ac:RestrictedPassword"/>
          </xs:choice>
        </xs:sequence>
        <xs:attribute name="preauth" type="xs:integer"
use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Authenticator" type="AuthenticatorType"/>

  <xs:complexType name="AuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthenticatorBaseType">
```

```
        <xs:choice>
          <xs:element ref="DigSig"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="DigSig" type="DigSigType"/>

  <xs:complexType name="DigSigType">
    <xs:complexContent>
      <xs:restriction base="ac:PublicKeyType">
        <xs:attribute name="keyValidation"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

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

  <xs:complexType name="ProtectedProtocolType">
    <xs:complexContent>
      <xs:restriction
base="ac:AuthenticatorTransportProtocolType">
        <xs:choice>
          <xs:element ref="ac:SSL"/>
          <xs:element ref="ac:WTLS"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.24 TimeSyncToken

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

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

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

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

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
  finalDefault="extension">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:ac"
schemaLocation="sstc-saml-schema-authn-context-1.0.xsd"/>

  <xs:annotation>
    <xs:documentation>
      urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
    </xs:documentation>
  </xs:annotation>
```

```
  <xs:complexType name="AuthnContextDeclaration">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="ac:Identification" minOccurs="0"/>
          <xs:element ref="ac:TechnicalProtection" minOccurs="0"/>
          <xs:element ref="ac:OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="ac:GoverningAgreements" minOccurs="0"/>
          <xs:element ref="ac:AuthenticatingAuthority" minOccurs="0"
            maxOccurs="unbounded"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="AuthnMethod" type="AuthnMethodType"/>

  <xs:complexType name="AuthnMethodType">
    <xs:complexContent>
      <xs:restriction base="ac:AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
          <xs:element ref="ac:Authenticator"/>
          <xs:element ref="ac:AuthenticatorTransportProtocol"
            minOccurs="0"/>
          <xs:element ref="ac:Extension" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="PrincipalAuthenticationMechanism"
type="TimeSyncMechType"/>

  <xs:complexType name="TimeSyncMechType">
    <xs:complexContent>
      <xs:restriction base="ac:PrincipalAuthenticationMechanismType">
        <xs:choice>
          <xs:element ref="Token"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="Token" type="TokenType"/>

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

  <xs:element name="TimeSyncToken" type="TimeSyncTokenType"/>

  <xs:complexType name="TimeSyncTokenType">
```

```
    <xs:complexContent>
      <xs:restriction base="ac:TimeSyncTokenType">

        <xs:attribute name="DeviceType" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="hardware"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>

        <xs:attribute name="SeedLength" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="64"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>

        <xs:attribute name="DeviceInHand" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="true"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

3.4.25 Unspecified

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

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

4 References

[RFC 1510] J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5).* IETF RFC 1510, September 1993. http://www.ietf.org/rfc/rfc1510.txt.

[RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[RFC 2945] T. Wu. *The SRP Authentication and Key Exchange System.* IETF RFC 2945, September 2000. http://www.ietf.org/rfc/rfc2945.txt.

[SAMLAC-xsd] J. Kemp et al., SAML authentication context schema. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-IP] J. Kemp et al., SAML context class schema for Internet Protocol. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-ip-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-IPP] J. Kemp et al., SAML context class schema for Internet Protocol Password. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-ippword-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-Kerb] J. Kemp et al., SAML context class schema for Kerberos. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-kerberos-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-MOFC] J. Kemp et al., SAML context class schema for Mobile One Factor Contract. Document ID sstc-saml-schema-authn-context-mobileonefactor-reg-1.0. See OASIS SSTC, August 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-MOFU] J. Kemp et al., SAML context class schema for Mobile One Factor Unregistered. Document ID sstc-saml-schema-authn-context-mobileonefactor-unreg-1.0. See OASIS SSTC, August 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-MTFC] J. Kemp et al., SAML context class schema for Mobile Two Factor Contract. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-mobiletwofactor-reg-1.0.See http://www.oasis-open.org/committees/security/.

[SAMLAC-MTFU] J. Kemp et al., SAML context class schema for Mobile Two Factor Unregistered. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-mobiletwofactor-unreg-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-Pass] J. Kemp et al., SAML context class schema for Password. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-pword-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-PGP] J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-pgp-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-PPT] J. Kemp et al., SAML context class schema for Password Protected Transport. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-ppt-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-Prev] J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-session-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-Smart] J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-smartcard-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SmPKI] J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-smartcardpki-1.0.

See http://www.oasis-open.org/committees/security/.

[SAMLAC-SPKI] J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-spki-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SRP] J. Kemp et al., SAML context class schema for Secure Remote Password. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-srp-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SSL] J. Kemp et al., SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-sslcert-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SwPKI] J. Kemp et al., SAML context class schema for Software PKI. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-softwarepki-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-Tele] J. Kemp et al., SAML context class schema for Telephony. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-telephony-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-TNom] J. Kemp et al., SAML context class schema for Telephony ("Nomadic"). OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-nomad-telephony-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-TPers] J. Kemp et al., SAML context class schema for Telephony (Personalized). OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-personal-telephony-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-TAuthn] J. Kemp et al., SAML context class schema for Telephony (Authenticated). OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-auth-telephony-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-TST] J. Kemp et al., SAML context class schema for Time Sync Token. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-timesync-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-X509] J. Kemp et al., SAML context class schema for Public Key – X.509. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-x509-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-XSig] J. Kemp et al., SAML context class schema for Public Key – XML Signature. OASIS SSTC, August 2004. Document ID sstc-saml-schema-authn-context-xmldsig-1.0. See http://www.oasis-open.org/committees/security/.

[SAMLCore] S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, August 2004. Document ID sstc-saml-core-2.0-cd-01. See http://www.oasis-open.org/committees/security/.

[Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures.* World Wide Web Consortium Recommendation, May 2001. http://www.w3.org/TR/xmlschema-1/.

[XMLSig] D. Eastlake et al., *XML-Signature Syntax and Processing*, World Wide Web Consortium, February 2002. http://www.w3.org/TR/xmldsig-core/.

Appendix A. Acknowledgments

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

- Conor Cahill, AOL
- Hal Lockhart, BEA Systems
- Rick Randall, Booz Allen Hamilton
- Ronald Jacobson, Computer Associates
- Gavenraj Sodhi, Computer Associates
- Tim Alsop, CyberSafe Limited
- Paul Madsen, Entrust
- Carolina Canales-Valenzuela, Ericsson
- Dana Kaufman, Forum Systems
- Irving Reid, Hewlett-Packard
- Paula Austel, IBM
- Maryann Hondo, IBM
- Michael McIntosh, IBM
- Anthony Nadalin, IBM
- Nick Ragouzis, Individual
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Prateek Mishra, Netegrity
- Forest Yin, Netegrity
- Peter Davis, Neustar
- Frederick Hirsch, Nokia
- John Kemp, Nokia
- Senthil Sengodan, Nokia
- Scott Kiester, Novell
- Steve Anderson, OpenNetwork
- Ari Kermaier, Oracle
- Vamsi Motukuru, Oracle
- Darren Platt, Ping Identity
- Jim Lien, RSA Security
- John Linn, RSA Security
- Rob Philpott, RSA Security
- Dipak Chopra, SAP
- Jahan Moreh, Sigaba
- Bhavna Bhatnagar, Sun Microsystems
- Jeff Hodges, Sun Microsystems
- Eve Maler, Sun Microsystems
- Ronald Monzillo, Sun Microsystems
- Emily Xu, Sun Microsystems
- Mike Beach, Boeing

- Greg Whitehead, Trustgenix
- James Vanderbeek, Vodafone

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

- Stephen Farrell, Baltimore Technologies
- David Orchard, BEA Systems
- Krishna Sankar, Cisco Systems
- Zahid Ahmed, CommerceOne
- Carlisle Adams, Entrust
- Tim Moses, Entrust
- Nigel Edwards, Hewlett-Packard
- Joe Pato, Hewlett-Packard
- Bob Blakley, IBM
- Marlena Erdos, IBM
- Marc Chanliau, Netegrity
- Chris McLaren, Netegrity
- Lynne Rosenthal, NIST
- Mark Skall, NIST
- Simon Godik, Overxeer
- Charles Norwood, SAIC
- Evan Prodromou, Securant
- Robert Griffin, RSA Security (former editor)
- Sai Allarvarpu, Sun Microsystems
- Chris Ferris, Sun Microsystems
- Emily Xu, Sun Microsystems
- Mike Myers, Traceroute Security
- Phillip Hallam-Baker, VeriSign (former editor)
- James Vanderbeek, Vodafone
- Mark O'Neill, Vordel
- Tony Palmer, Vordel

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

- Thomas Gross, IBM
- Birgit Pfitzmann, IBM

Appendix B. Notices

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

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