SIGNICAT
Digital Identity On Demand

Long Time Validation extended Signed Data Object

Specification of version 1.1

Document version 1.0:

Table of Contents

Document history

Document version	Date	Change
0.5	17.01.2014	Document created from policy version 1.1, document version 1.0
0.6	17.10.2014	Added descriptions of OriginalDocument and BundleIndex.
1.0	1.11.2014	Released as document version 1.0

References

Short name	Reference
CAdES	ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".
XAdES	ETSI TS 101 903: “XML Advanced Electronic Signatures (XAdES)
PAdES	ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles

Introduction

Following the European Commission (EC) Electronic Signature Directive 1999/93/EC, ETSI[1] developed standards for e-signatures that fulfilled the requirements for “advanced” and “qualified” e-signatures in the directive. These three related standards, named CAdES, XAdES and PAdES, define e-signature formats for CMS-, XML- and PDF-based signatures. A major concern for these standards has been the ability to validate signatures many years after the signing took place, also known as “long-term validation” (LTV).

During the following decade many e-signature solutions have been widely deployed in Scandinavia. Only a very few of those support the *AdES standards, and none of them use these standards for the default e-signature format. Typically they produce e-signatures on standards like XML Digital Signature, CMS/PKCS#7 or similar, proprietary standards.

This situation, where all e-ID solutions produce signatures on different formats, complicates the usage of e-signatures, because it is often not desirable to require that all signers use the same e-signature solution.

The support for long-term validation of e-signatures is similarly varying, and often lacking completely. Signature formats like XML Signature and CMS/PKCS#7 do not support verification of the signature after the signing certificate is expired or revoked. Worse, it is impossible to securely determine when the signature was created without relying on external evidence like secure logs and similar.

A signature verifier could extend an e-signature with long-time validation support, but typically the e-signature does not support the inclusion of the necessary data elements. The *AdES standards cannot be used, because they require that the original signature producing software created the signature on *AdES format from the start.

This document defines an e-signature storage format that can be part of a solution to the problems described above. The signature format extends a digital signature with long-time validation support, even if the original digital signature format did not support this. It also provides a uniform signature format that can contain e-signatures produced with different e-ID solutions.

1European Telecommunications Standard Institute

Requirements

The main requirements to the format are:

A common storage format for e-signatures that can be applied after the signature has been created, and which does not need support from the signature creation software. The format needs to be flexible enough to support different native e-signature formats, like XML Digital Signature, CMS/PKCS#7 and others.

Consistent support for validation of e-signatures originating from different e-signature services. The format should support the inclusion of validation data and a packaging policy specification to obtain a consistent support for validation for all e-signatures used in a specific application.

Support for long-time validation. The format should support inclusion of validation data and time stamps to make e-signatures suited for long-time validation and storage.

Support for signature context information. The context in which a signature was created may be of great significance for assessing the strength of a signature. The signature creation environment and the application context are important to understand how the information and act of signing was presented to the signer. Apart from that, all recorded details can function as additional evidence, and potentially further strengthen non-repudiation.

Support for audit trails. The audit trails show the history of the e-signature. They add evidence and strengthen non-repudiation.

Standards based. The format should build on existing standards as far as possible. Specifically, the LTV support is aligned with the *AdES standards. The *AdES standards are designed to comply with the European legal framework, and their support for long-time validation is recognized.

Format structure

An LTV-SDO consists of five main elements:

1. The packaging policy identifier identifies the packaging policy, which defines how the package was created, and how it can be verified and used.
2. The native signature contains the e-signature we are primarily interested in, the one we want to affirm. It also may contain validation data, which facilitates validation of this signature, like revocation information or certificates.
3. The signature context contains information about the context in which the original signature was created, like software versions and references to the application context.
4. The audit trails are secure logs of the creation and verification of the signature.
5. The TSP signature is a digital signature made on the complete LTV-SDO by a Trusted Service Provider to secure its integrity and authenticity. Specifically, the qualifying properties for the native signature, the signature context information and the audit trail are signed by the TSP signature.

Major parties

The major parties involved in the processes using the LTV-SDO are mainly the same as in XAdES, the most important being the Signer, the Verifier and the Time-Stamping Authority. A new role is defined for a trusted party which collects signature context information and validation data, and formats and signs the LTV-SDO. It is simply called the TSP (Trusted Service Provider). The TSP typically also covers the Verifier role, but not necessarily.

The packaging policy

In the *AdES standards, a signature policy is defined as “a set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid.”

The native signature may or may not have an explicit or implicit signature policy. This signature policy may or may not be identified in the native SDO.

This is potentially a problem for long time validation. The verifier needs to know how to validate the signature. Also, as the LTV-SDO adds support for additional validation data, there is a need for defining how this support should be used for a given type of native SDO and a given context.

To this end a separate policy, called a *packaging policy*, is defined for the creation and verification of an LTV-SDO.

The purpose of the packaging policy is to specify requirements for the packaging process, and high-level requirements for the prior signature creation and verification process.

The primary users of the packaging policy will be e-signature users (relying parties). The policy will help e-signature users to better understand the information contained in a package, and on what basis it can be trusted and used.

The policy will also be useful for implementers of the packaging service.

The packaging policy may refer to native SDO signature policies, or other normative documentation, that helps to define the creation and verification process.

The TSP Signature

As described in the *AdES standards, most of the validation data can be added by the verifier after the signature has been created. It is sufficient that these validation data are available, hence no integrity protection is needed. For validation data which need integrity protection, e. g. the signing certificate, the *AdES standards require them to be signed by the signatory. This requires support from the native signature client, which cannot be presupposed. The LTV-SDO supports additional evidence in the form of signature context and audit trails, for which authenticity and integrity need to be protected.

The requirement for protection of validation data is met by supporting a signature performed by a Trusted Service Provider (TSP) over all validation data. The Trusted Service Provider may do this in connection with the signature creation or verification, this will typically be described in the packaging policy.

Validation data

The general strategy for incorporating validation data into the LTV-SDO is to use the mechanisms defined in XAdES as far as possible.

XAdES adds “qualifying properties” to an XMLDSIG signature. Some of these are signed by the signer, and others are unsigned. Similarly, the LTV-SDO adds strength to various e-signature formats by adding exactly the same type of qualifying properties. The main difference is that the LTV-SDO does not require that any of the qualifying properties are signed by the signer. Instead they are signed by the TSP.

This has two implications for verification of the original signature: First, the verifier needs to verify the TSP signature in addition to the original signature. The TSP signature is an ordinary XAdES, so this can be done through the normal XAdES mechanisms.

Second, the verifier must rely on the TSP signature instead of the original signature for the correctness of the signed qualifying properties.

Time-stamping

Time-stamping can be done by a standard XAdES archive time-stamp on the TSP signature. Because an archive time-stamp also covers the signed data, the contained native signature will be covered.

Additionally, it is possible to use a XAdES Data Object time stamp to time-stamp only the signed data. This time-stamp will be covered by the TSP signature.

Process descriptions

The next two sections illustrate the LTV-SDO structure through a process perspective.

Package Evolution

This section shows how a typical LTV-SDO package may evolve. The details of the process are defined by the chosen packaging policy.

1. TSP determines packaging policy

The signature policy is typically agreed upon in advance, or implied.

2. TSP collects signature context information

The TSP collects the signature context information.

3. Signer generates signature

The Signer generates the signature.

4. Verifier verifies the signature and collects validation data

The verifier verifies the original signature. The validation data used in this verification are collected and passed to the TSP, which adds them to the LTV-SDO.

5. TSP collects additional data

The TSP collects additional data and adds them to the LTV-SDO.

6. TSP signs the LTV-SDO

The TSP signs the LTV-SDO. Validation data are collected, and added to the LTV-SDO.

7. TSA time stamps the original signature (optional)

A Time Stamping Authority (TSA) creates a time stamp over the TSP signature and all data signed by the TSP, including the native signature and the signature context. The time stamp will also cover validation data for the TSP signature.

8. (Later) TSA time stamps the LTV-SDO

After some time, a Time Stamping Authority (TSA) stamps the LTV-SDO and the original signature to strengthen the cryptography and/or protect against key compromise. This step may be repeated.

Signature Verification Process

This section shows how a typical LTV-SDO signature is verified. The details of the process are defined by the signature policy identified in the signature.

1. TSP determines signature policy

The signature policy is typically agreed upon in advance, or implied.

2. The most recent archive time stamp is validated.

The most recent archive time stamp is validated in respect to the verification time. The validation process conforms to XAdES.

3. Any previous time stamps are validated

Any previous time stamps are validated with respect to the time of the immediate following time stamp. This step is repeated for all archive time stamps. The validation process conforms to XAdES.

4. The TSP signature is validated

The signature validation process is described by XAdES.

5. The native signature is validated

The native signature is validated. How this is done, depends on the native signature, and is described in the signature policy.

Description of XML elements

This section describes the main XML elements in the LTV-SDO format.

LtvSdo
This is the root element, which contains the complete LTV-SDO.

Consists of: Description, PackagingPolicyIdentifier, NativeSignature, AdditionalInfo, SignatureContext, AuditTrails and Signature.

Description
Provides an accessible description of the LTV-SDO.

Consists of: SignerDescription, DocumentDescription and SignatureDescription

SignerDescription
Description of the signer.

Consists of: SignerDisplayName, SignerUniqueId, SignerNationalId, SignerNationality, signerNationalIdType, and other Attributes

DocumentDescription
Description of the signed document.

Consists of: DocumentMimeType, DocumentTitle, DocumentDigest

SignatureDescription
Description of the signature.

Consists of: SignatureTypeFriendlyName, SignatureFormatFriendlyName, SigningTime

PackagingPolicyIdentifier
Identifies the packaging policy, which describes how the package was created, rules for the formatting of the package, and how the package can be validated.

NativeSignature
Contains the original signature made by the signer on the document or data.

Consists of: NativeSdo¸ NativeSignatureQualifyingProperties.

NativeSdo
The Signed Data Object containing the original signature, and often the original documents and some validation data. The attributes “Format”and “MimeType” specifies the SDO format and MIME-type.

NativeSignatureQualifyingProperties
Data that facilitate validation of the native signature. This element is similar to the XAdES QualifyingProperties element, but without the distinction between signed and unsigned properties.

BundleIndex
Present when this LtvSdo is part of a document-bundle signature. Contains the index into the bundle of the signed document represented by this LtvSdo.

OriginalDocument
The original, unsigned document. Used if the original document is not included in the NativeSdo.

AdditionalInfo
Additional information added to the package by the TSP.

Consists of: SignerAttributes

SignatureContext
Information about the context in which the original signature was created.

Consists of: SignatureCreationContext, SignatureVerificationContext and ExternalContext.

SignatureCreationContext
Describes the technical environment the signature was created in. Typically, it identifies software names and versions used for signature creation.

SignatureVerificationContext
Describes the technical environment the signature was verified in. Typically, it identifies software names and versions used for signature verification.

ExternalContext
Contains a reference to the external context in which this signature was created. This could for example be a reference to the business transaction which uses the signature.

AuditTrails
Contains records of the most important events in the creation and verification of the signature.

Consists of: SignatureCreationAuditTrail, SignatureVerificationAuditTrail

SignatureCreationAuditTrail
Contains records of the most important events in the creation of the signature.

It may also include details about the client configuration, such as the IP address.

SignatureVerificationAuditTrail
Contains records of the most important events in the verification of the signature.

Signature

Contains the TSP signature in XAdES format.

Annex A: Example LTV-SDO

The following is an example LTV-SDO, included to illustrate the format in use.

Note that several values are shortened for readability, and that the formats of identifiers, log entries and similar may be different in a real-world application.

```
<?xml version="1.0" encoding="UTF-8"?>
<ltv:LtvSdo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:ltv="https://id.signicat.com/definitions/xsd/LtvSdo-1.0"
            xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Id="root">
    <ltv:Description>
        <ltv:SignerDescription>
            <ltv:SignerDisplayName>Pseudonym</ltv:SignerDisplayName>
            <ltv:SignerUniqueId>9208-2002-2-207175795269</ltv:SignerUniqueId>
            <ltv:SignerNationalId>1112703751</ltv:SignerNationalId>
            <ltv:SignerNationality>DK</ltv:SignerNationality>
            <ltv:SignerNationalIdType>CPR</ltv:SignerNationalIdType>
            <ltv:Attribute Name="unique-id" NameSpace="nemid">9208-2002-2-
207175795269</ltv:Attribute>
            <ltv:Attribute Name="subject-dn" NameSpace="nemid">
                CN=Pseudonym+serialnumber=PID:9208-2002-2-207175795269,O=Ingen
organisatorisk tilknytning,C=DK
            </ltv:Attribute>
            <ltv:Attribute Name="cpr" NameSpace="nemid">1112703751</ltv:Attribute>
            <ltv:Attribute Name="serialnumber"
NameSpace="nemid">1275249435</ltv:Attribute>
            <ltv:Attribute Name="issuer-dn" NameSpace="nemid">CN=TRUST2408 Systemtest
VIII CA, O=TRUST2408, C=DK
            </ltv:Attribute>
        </ltv:SignerDescription>
        <ltv:DocumentDescription>
            <ltv:DocumentMimeType>application/pdf</ltv:DocumentMimeType>
            <ltv:DocumentTitle>Aksept</ltv:DocumentTitle>
            <ltv:DocumentDigest alg="http://www.w3.org/2001/04/xmlenc#sha256">
                DTEifuOt60mWYy8WaS00THvM3VizLZMu5ysGMhnw3R4=
            </ltv:DocumentDigest>
        </ltv:DocumentDescription>
```

```
        <ltv:SignatureDescription>
            <ltv:SignatureTypeFriendlyName>NemID</ltv:SignatureTypeFriendlyName>
            <ltv:SignatureFormatFriendlyName>XML
Signature</ltv:SignatureFormatFriendlyName>
            <xades:SigningTime>2013-02-23T12:03:34.000+01:00</xades:SigningTime>
        </ltv:SignatureDescription>
    </ltv:Description>

<ltv:PackagingPolicyIdentifier>urn:signicat:packagingpolicy:ltv:nemid:1.0:1.0</ltv:Packag
ingPolicyIdentifier>
    <ltv:NativeSignature>
        <ltv:NativeSdo Format="urn:ksi:names:SAML:2.0:df:xmldsig"
MimeType="application/x-xml-dsig" Version="1.0">
            PD94bWwgdmVyc2lvbj0iMS4(...)uYXR1cmU+
        </ltv:NativeSdo>
        <ltv:NativeSignatureQualifyingProperties>
            <xades:SigningTime>2013-02-23T12:04:05.411+01:00</xades:SigningTime>
            <xades:RevocationValues>
                <xades:CRLValues>

<xades:EncapsulatedCRLValue>MIICy(...)nE5ixI0bdO9An5mTw==</xades:EncapsulatedCRLValue>
                </xades:CRLValues>
                <xades:OCSPValues>

<xades:EncapsulatedOCSPValue>MIIHSzCB(...)YZmftsPRI/WSvvPw=</xades:EncapsulatedOCSPValue>
                </xades:OCSPValues>
            </xades:RevocationValues>
        </ltv:NativeSignatureQualifyingProperties>
    </ltv:NativeSignature>
    <ltv:AdditionalInfo>
        <ltv:SignerAttributes>
            <ltv:Attribute Name="pidCprReply"
NameSpace="nemid">PHNv(...)W52ZWxvcGU+</ltv:Attribute>
        </ltv:SignerAttributes>
    </ltv:AdditionalInfo>
    <ltv:SignatureContext>
        <ltv:SignatureCreationContext Type="nemid">
            <ltv:Component Name="server-os" Version="Linux-2.6.18-164.2.1.el5"/>
            <ltv:Component Name="DocumentViewerModule" Version="1.3.9"/>
            <ltv:Component Name="server-java" Version="Sun Microsystems Inc.-1.6.0_37"/>
```

```
            <ltv:Component Name="DocumentProviderModule" Version="1.3.9"/>
            <ltv:Component Name="NemIdModule" Version="2.4.4-SNAPSHOT"/>
            <ltv:Component Name="user-agent"
                           Version="Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:19.0)
Gecko/20100101 Firefox/19.0"/>
            <ltv:Component Name="DetectorModule" Version="2.2.4"/>
            <ltv:Component Name="Signicat Services Portal" Version="1.16.0"/>
            <ltv:Component Name="client-java" Version="1.7.0_15"/>
        </ltv:SignatureCreationContext>
        <ltv:SignatureVerificationContext Type="nemid">
            <ltv:Component Name="server-os" Version="Linux-2.6.18-164.2.1.el5"/>
            <ltv:Component Name="ooapi" Version="ooapi-signicat-custom-1.81.3.V4.jar"/>
            <ltv:Component Name="server-java" Version="Sun Microsystems Inc.-1.6.0_37"/>
            <ltv:Component Name="NemIdModule" Version="2.4.4-SNAPSHOT"/>
            <ltv:Component Name="Signicat Services Portal" Version="1.16.0"/>
        </ltv:SignatureVerificationContext>
        <ltv:ExternalContext>
            <ltv:ExternalReference>This is the external reference</ltv:ExternalReference>
        </ltv:ExternalContext>
    </ltv:SignatureContext>
    <ltv:AuditTrails>
        <ltv:SignatureCreationAuditTrail>
            (omitted)
        </ltv:SignatureCreationAuditTrail>
        <ltv:SignatureVerificationAuditTrail>
            (omitted)
        </ltv:SignatureVerificationAuditTrail>
    </ltv:AuditTrails>
    <ds:Signature Id="xmldsig-c00c04bd-00cc-4dd5-ab26-a5316f308424"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
            <ds:Reference Id="xmldsig-c00c04bd-00cc-4dd5-ab26-a5316f308424-ref0"
URI="#root">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
```

```
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>UUT0MEhhOvQ2HsANGbgO3+HgANuAqfEh/7MA5+jUsLQ=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
                          URI="#xmldsig-c00c04bd-00cc-4dd5-ab26-a5316f308424-
signedprops">
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>gtpFIa2Y2zBTJIPQNaf3KS8ewAprCFxYcwFowZh98fY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue Id="xmldsig-c00c04bd-00cc-4dd5-ab26-a5316f308424-sigvalue">
            ThUoeVI(...)0TseMWT/9g==
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>
                    MIIEm(...)jwcek=
                </ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
        <ds:Object>
            <xades:QualifyingProperties
xmlns:xades141="http://uri.etsi.org/01903/v1.4.1#"
                                        Target="#xmldsig-c00c04bd-00cc-4dd5-ab26-
a5316f308424"
                                        xmlns:xades="http://uri.etsi.org/01903/v1.3.2#">
                <xades:SignedProperties Id="xmldsig-c00c04bd-00cc-4dd5-ab26-a5316f308424-
signedprops">
                    <xades:SignedSignatureProperties>
                        <xades:SigningTime>2013-02-
23T12:04:05.795+01:00</xades:SigningTime>
                        <xades:SigningCertificate>
                            <xades:Cert>
                                <xades:CertDigest>
                                    <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>BNefJx2p3KXrapT9vjuviJ7BwNdUFID2mKp36R5UV5c=</ds:DigestValue>
```

```
                                </xades:CertDigest>
                                <xades:IssuerSerial>
                                    <ds:X509IssuerName>CN=Buypass Class 3 Test4 CA
1,O=Buypass,C=NO</ds:X509IssuerName>

<ds:X509SerialNumber>269856267150500156063753</ds:X509SerialNumber>
                                </xades:IssuerSerial>
                            </xades:Cert>
                            <xades:Cert>
                                <xades:CertDigest>
                                    <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>+lWn7dbCYHG8ZOw/PiDdjw18toH/4vmjrLgTYgY3Cj8=</ds:DigestValue>
                                </xades:CertDigest>
                                <xades:IssuerSerial>
                                    <ds:X509IssuerName>CN=Buypass Class 3 Test4 CA
1,O=Buypass,C=NO</ds:X509IssuerName>
                                    <ds:X509SerialNumber>1</ds:X509SerialNumber>
                                </xades:IssuerSerial>
                            </xades:Cert>
                        </xades:SigningCertificate>
                    </xades:SignedSignatureProperties>
                </xades:SignedProperties>
                <xades:UnsignedProperties>
                    <xades:UnsignedSignatureProperties>
                        <xades:CertificateValues>

<xades:EncapsulatedX509Certificate>MIIDQTCC(...)8iu3q</xades:EncapsulatedX509Certificate>
                        </xades:CertificateValues>
                        <xades:RevocationValues>
                            <xades:OCSPValues>

<xades:EncapsulatedOCSPValue>MIICDQoBAK(...)VJcUTg==</xades:EncapsulatedOCSPValue>
                            </xades:OCSPValues>
                        </xades:RevocationValues>
                    </xades:UnsignedSignatureProperties>
                </xades:UnsignedProperties>
            </xades:QualifyingProperties>
        </ds:Object>
```

```
    </ds:Signature>
</ltv:LtvSdo>
```

Annex B: LTV-SDO Schema

```
<?xml version="1.0" encoding="iso-8859-1"?>
<xs:schema xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
           xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
           xmlns:xs="http://www.w3.org/2001/XMLSchema"
           targetNamespace="https://id.signicat.com/definitions/xsd/LtvSdo-1.0"
           xmlns="https://id.signicat.com/definitions/xsd/LtvSdo-1.0"
           elementFormDefault="qualified">

    <xs:import namespace="http://uri.etsi.org/01903/v1.3.2#" schemaLocation="XAdES.xsd"/>
    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"/>

    <xs:element name="LtvSdo" type="LtvSdoType"/>

    <xs:complexType name="LtvSdoType">
        <xs:sequence>
            <xs:element name="Description" type="DescriptionType" nillable="false"
minOccurs="1" maxOccurs="1"/>
            <xs:element name="PackagingPolicyIdentifier" type="xs:string"  minOccurs="1"
maxOccurs="1"/>
            <xs:element name="NativeSignature" type="NativeSignatureType"
nillable="false" minOccurs="1" maxOccurs="1"/>
            <xs:element name="AdditionalInfo" type="AdditionalInfoType" nillable="false"
minOccurs="0" maxOccurs="1"/>
            <xs:element name="SignatureContext" type="SignatureContextType"
nillable="false" minOccurs="0" maxOccurs="1"/>
            <xs:element name="AuditTrails" type="AuditTrailsType" nillable="false"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ds:Signature" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
        <xs:attribute name="Id" type="xs:string"/>
    </xs:complexType>

    <xs:complexType name="DescriptionType">
        <xs:sequence>
            <xs:element name="SignerDescription" type="SignerDescriptionType"
nillable="false" minOccurs="1" maxOccurs="1"/>
```

```
            <xs:element name="DocumentDescription" type="DocumentDescriptionType"
nillable="false" minOccurs="1" maxOccurs="1"/>
            <xs:element name="SignatureDescription" type="SignatureDescriptionType"
nillable="false" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="SignerDescriptionType">
        <xs:sequence>
            <xs:element name="SignerDisplayName" type="xs:string" nillable="false"
minOccurs="1" maxOccurs="1"/>
            <xs:element name="SignerUniqueId" type="xs:string" nillable="false"
minOccurs="0" maxOccurs="1"/>
            <xs:element name="SignerNationalId" type="xs:string" nillable="false"
minOccurs="0" maxOccurs="1"/>
            <xs:element name="SignerNationality" type="xs:string" nillable="false"
minOccurs="0" maxOccurs="1"/>
            <xs:element name="SignerNationalIdType" type="xs:string" nillable="false"
minOccurs="0" maxOccurs="1"/>
            <xs:element name="Attribute" type="AttributeType" nillable="false"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="DocumentDescriptionType">
        <xs:sequence>
            <xs:element name="DocumentMimeType" type="xs:string" nillable="false"
minOccurs="1" maxOccurs="1"/>
            <xs:element name="DocumentTitle" type="xs:string" nillable="false"
minOccurs="1" maxOccurs="1"/>
            <xs:element name="DocumentDigest" type="DocumentDigestType" nillable="false"
minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="DocumentDigestType">
        <xs:simpleContent>
            <xs:extension base="xs:base64Binary">
                <xs:attribute name="alg" type="xs:anyURI"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
```

```
    <xs:complexType name="SignatureDescriptionType">
        <xs:sequence>
            <xs:element name="SignatureTypeFriendlyName" type="xs:string"
nillable="false" minOccurs="1" maxOccurs="1"/>
            <xs:element name="SignatureFormatFriendlyName" type="xs:string"
nillable="false" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="xades:SigningTime" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="NativeSignatureType">
        <xs:sequence>
            <xs:element name="NativeSdo" type="NativeSdoType" nillable="false"
minOccurs="1" maxOccurs="1"/>
            <xs:element name="NativeSignatureQualifyingProperties"
type="NativeSignatureQualifyingPropertiesType" nillable="false" minOccurs="0"
maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="SignatureContextType">
        <xs:sequence>
            <xs:element name="SignatureCreationContext"
type="SignatureCreationOrVerificationContextType" nillable="false" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="SignatureVerificationContext"
type="SignatureCreationOrVerificationContextType" nillable="false" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="ExternalContext" type="ExternalContextType"
nillable="false" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="AuditTrailsType">
        <xs:sequence>
            <xs:element name="SignatureCreationAuditTrail"
type="SignatureCreationOrVerificationAuditTrailType" nillable="false" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="SignatureVerificationAuditTrail"
type="SignatureCreationOrVerificationAuditTrailType" nillable="false" minOccurs="0"
maxOccurs="1"/>
        </xs:sequence>
```

```
    </xs:complexType>

    <xs:complexType name="NativeSdoType">
        <xs:simpleContent>
            <xs:extension base="xs:base64Binary">
                <xs:attribute name="Format" type="xs:string"/>
                <xs:attribute name="MimeType" type="xs:string"/>
                <xs:attribute name="Version" type="xs:string"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>

    <xs:complexType name="NativeSignatureQualifyingPropertiesType">
        <xs:sequence>
            <xs:element ref="xades:SigningTime" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="xades:SigningCertificate" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="xades:CertificateValues" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="xades:RevocationValues" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="SignatureCreationOrVerificationContextType">
        <xs:sequence>
            <xs:element name="Component" type="ComponentType" minOccurs="1"
maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Type" type="xs:string"/>
    </xs:complexType>

    <xs:complexType name="ExternalContextType">
        <xs:sequence>
            <xs:element name="ExternalReference" type="xs:string" minOccurs="1"
maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="SignatureCreationOrVerificationAuditTrailType">
        <xs:sequence>
            <xs:element name="Event" type="EventType" minOccurs="1"
```

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

    <xs:complexType name="ComponentType">
        <xs:attribute name="Name" type="xs:string"/>
        <xs:attribute name="Version" type="xs:string"/>
    </xs:complexType>

    <xs:complexType name="EventType">
        <xs:sequence>
            <xs:element name="Timestamp" type="xs:dateTime" nillable="false"
minOccurs="1" maxOccurs="1"/>
            <xs:element name="Type" type="xs:string" nillable="false" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="Data" type="DataType" nillable="false" minOccurs="1"
maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="DataType">
        <xs:sequence>
            <xs:element name="DataEntry" type="DataEntryType" minOccurs="1"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="DataEntryType">
        <xs:simpleContent>
            <xs:extension base="xs:string">
                <xs:attribute name="Name" type="xs:string"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>

    <xs:complexType name="AdditionalInfoType">
        <xs:sequence>
            <xs:element name="SignerAttributes" type="SignerAttributeType"
nillable="false" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
```

```
    </xs:complexType>

    <xs:complexType name="SignerAttributeType">
        <xs:sequence>
            <xs:element name="Attribute" type="AttributeType" minOccurs="1"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="AttributeType">
        <xs:simpleContent>
            <xs:extension base="xs:anySimpleType">
                <xs:attribute name="NameSpace" type="xs:string"/>
                <xs:attribute name="Name" type="xs:string"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
</xs:schema>
```