ETSI TS 119 102-2 V1.1.1 (2018-08)

Electronic Signatures and Infrastructures (ESI);
Procedures for Creation and Validation of
AdES Digital Signatures;
Part 2: Signature Validation Report

Reference
DTS/ESI-0019102-2

Keywords
electronic signature, trust services, validation

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 2 of a multi-part deliverable covering Procedures for Creation and Validation of AdES Digital Signatures, as identified below:

Part 1: "Creation and Validation";

Part 2: "Signature Validation Report".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies a general structure and an XML format for reporting the validation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.1], ETSI EN 319 132-1 [4], ETSI EN 319 142-1 [i.3] respectively). The present document is aligned with the requirements specified in ETSI TS 119 102-1 [1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[2] W3C Recommendation: "XML-Signature Syntax and Processing Version 1.1", D. Eastlake et al., April 2013.

NOTE: Available at http://www.w3.org/TR/xmldsig-core/.

[3] ETSI TS 101 903 (V1.3.2): "XML Advanced Electronic Signatures (XAdES)".

[4] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[5] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[6] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[8] IETF RFC 3061: "A URN Namespace of Object Identifiers".

[9] ISO 32000-1:2008: "Document management - Portable document format - Part 1: PDF 1.7".

[10] W3C Recommendation: "XML Schema Definition Language (XSD) 1.1 Part 1: Structures".

NOTE: Available at https://www.w3.org/TR/xmlschema11-1/.

[11] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[12] IETF RFC 5035: "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.2] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.3] ETSI EN 319 142-1: "ETSI EN 319 142 1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.4] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.6] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.7] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.8] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.9] Recommendation ITU-R TF.460-6: "Standard-frequency and time-signal emissions".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

AdES (digital) signature: digital signature that is either a CAdES signature, or a PAdES signature or a XAdES signature

advanced electronic signature: As defined in Regulation (EU) No 910/2014 [i.8].

CAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 122-1 [i.1] or ETSI EN 319 122-2 [i.2]

certificate: See public key certificate.

certificate revocation list: signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

claimed signing time: time of signing claimed by the signer which on its own does not provide independent evidence of the actual signing time

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [i.9]

data object: actual binary/octet data being operated on (transformed, digested, or signed) by an application

data to be signed formatted: data created from the data to be signed objects by formatting them and placing them in the correct sequence for the computation of the data to be signed representation

data to be signed representation: hash of the data to be signed formatted, which is used to compute the digital signature value

digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

digital signature value: result of the cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

evidence record: unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time

NOTE: See IETF RFC 4998 [i.6] and IETF RFC 6283 [i.7].

PAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 142-1 [i.3] or ETSI EN 319 142-2 [i.4]

proof of existence: evidence that proves that an object existed at a specific date/time

public key: in a public key cryptographic system, that key of an entity's key pair which is publicly known

public key certificate: public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it

qualified electronic signature: As defined in Regulation (EU) No 910/2014 [i.8].

signature attribute: signature property

signature validation application: application that validates a signature against a signature validation policy, and that outputs a status indication (i.e. the signature validation status) and a signature validation report

NOTE: The signature validation application (SVA) is specified in ETSI TS 119 102-1 [1].

signature validation constraint: technical criteria against which a digital signature can be validated, e.g. as specified in ETSI TS 119 102-1 [1].

signature validation policy: set of signature validation constraints processed or to be processed by the signature validation application

signature validation report: comprehensive report of the validation provided by the signature validation application to the driving application and allowing the driving application, and any party beyond the driving application, to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the signature validation application

NOTE: Clause 5.1.3 of ETSI TS 119 102-1 [1] specifies minimum requirements for the content of such a report.

signature validation status: One of the following indications: TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE.

signature validation: process of verifying and confirming that a digital signature is technically valid

signer: entity being the creator of a digital signature

(electronic) time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

trusted list: list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation

NOTE: In the context of European Union Member States, as specified in Regulation (EU) No 910/2014 [i.8], it refers to an EU Member State list including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

In the context of non-EU countries or international organizations, it refers to a list meeting the requirements of ETSI TS 119 612 [6] and providing assessment scheme based approval status information about trust services from trust service providers, for compliance with the relevant provisions of the applicable approval scheme and the relevant legislation.

XAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 132-1 [4] or ETSI EN 319 132-2 [5]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AdES	Advanced Electronic Signature
CRL	Certificate Revocation List
DA	Driving Application
DSS	Digital Signature Service
DTBSF	Data To Be Signed Formatted
DTBSR	Data To Be Signed Representation
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
POE	Proof Of Existence
SD	Signer's Document
SDR	Signer's Document Representation
SVA	Signature Validation Application
TSP	Trust Service Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
VRI	Validation Related Information
W3C	World Wide Web Consortium
XML	eXtensible Markup Language

4 Signature Validation Report Structure

4.1 General provisions

4.1.1 Report Structure

4.1.1.1 General

The present document defines the structure of reporting the result of the validation of an AdES digital signature (specified in ETSI EN 319 122-1 [i.1], ETSI EN 319 132-1 [4], ETSI EN 319 142-1 [i.3] respectively). The signature validation application (SVA) is assumed to follow the signature validation model specified in ETSI TS 119 102-1 [1] and illustrated by Figure 1.

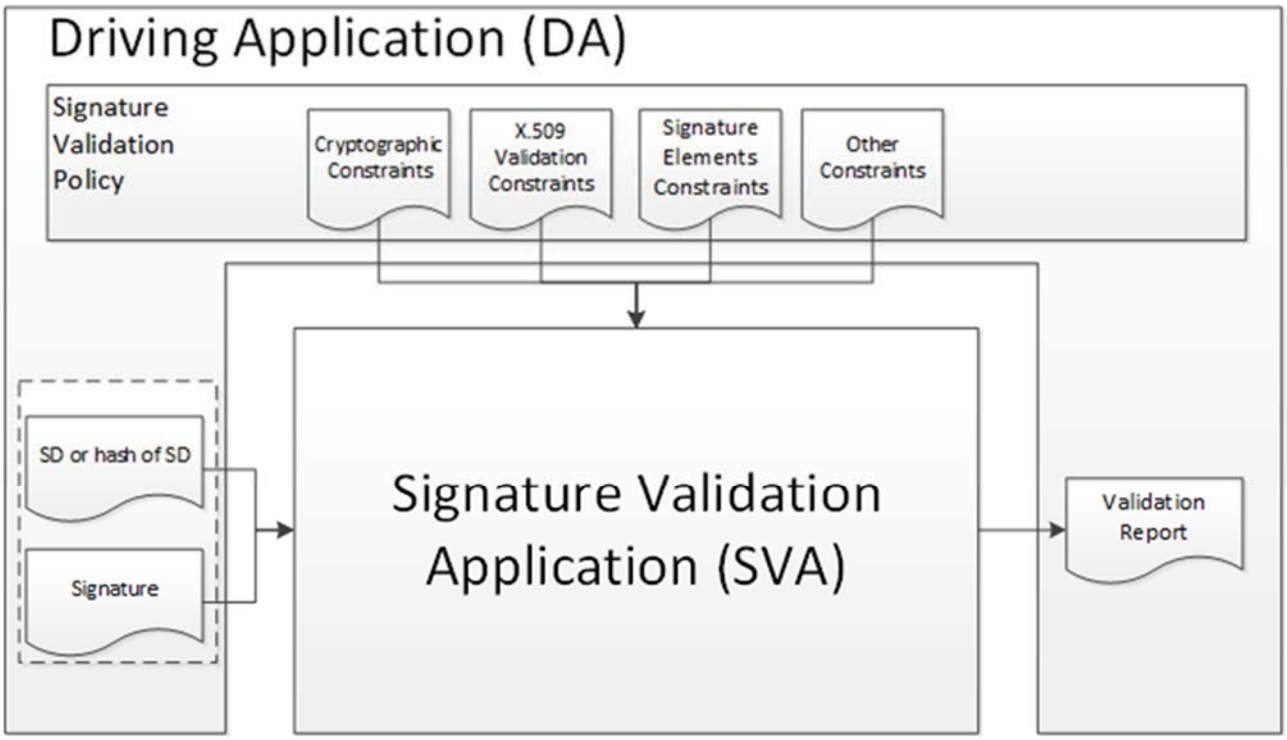

Figure 1: Conceptual Model of Signature Validation ETSI EN 119 102-1 [1]

The signature validation report shall consist of:

- One or more S*ignature Validation Report*-elements, each element containing the overall signature validation status for one signature as well as additional information on the signature validation performed. Clause 4.3 describes this element.

It may also contain:

- A S*ignature Validation Objects*-element, containing objects used during validation, such as trust anchors, CRLs, or time-stamps. Clause 4.4 describes this element.

NOTE: Objects contained in a signature validation objects element can be trust anchor information, CRLs or time-stamps. Some of these objects tend to be large. The signature validation objects element acts a container allowing storing objects only once even when they are needed for more than one signature validation report element.

- A *Validator Information Element*, containing information on the entity validating the signature(s) and producing the report. Clause 4.5 describes this element.

- A *Validation Report Signature Element*, containing a signature on the report. Clause 4.6 describes this element.

Figure 2 illustrates this structure. Figure 3 shows the structure with the elements contained in each of the fields. The following clauses describe these elements.

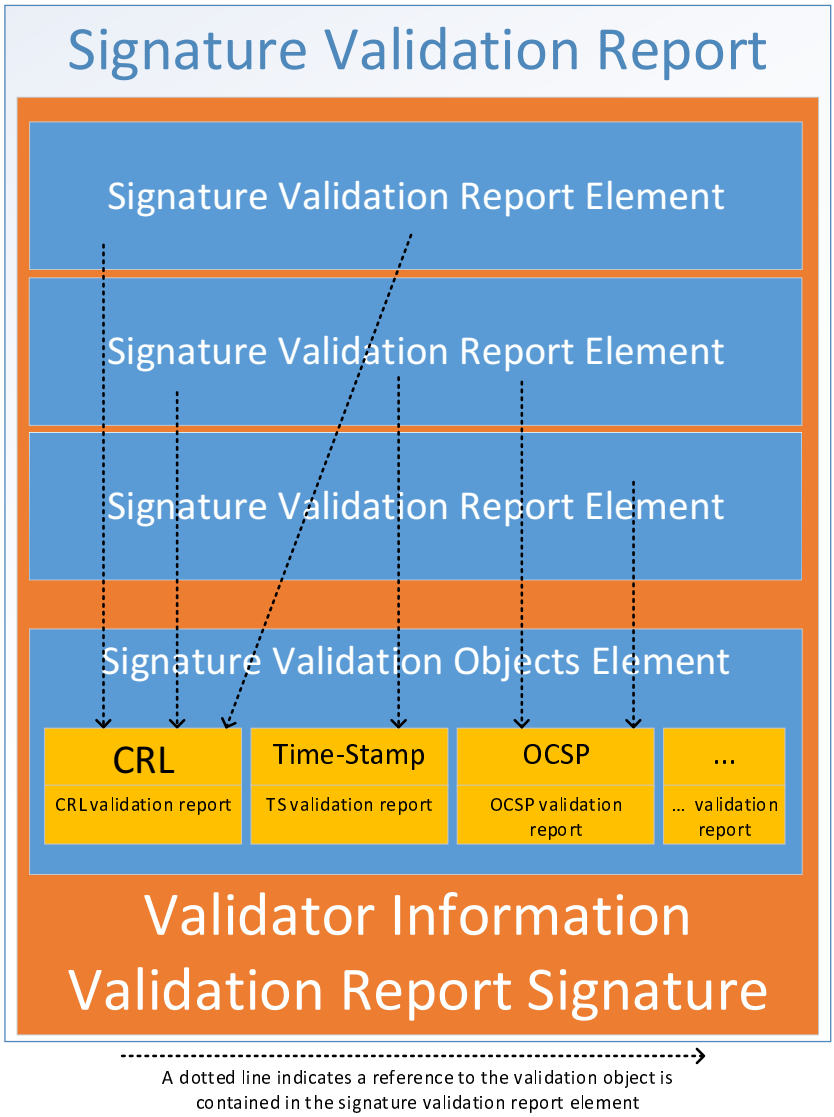

Figure 2: Signature Validation Report Structure

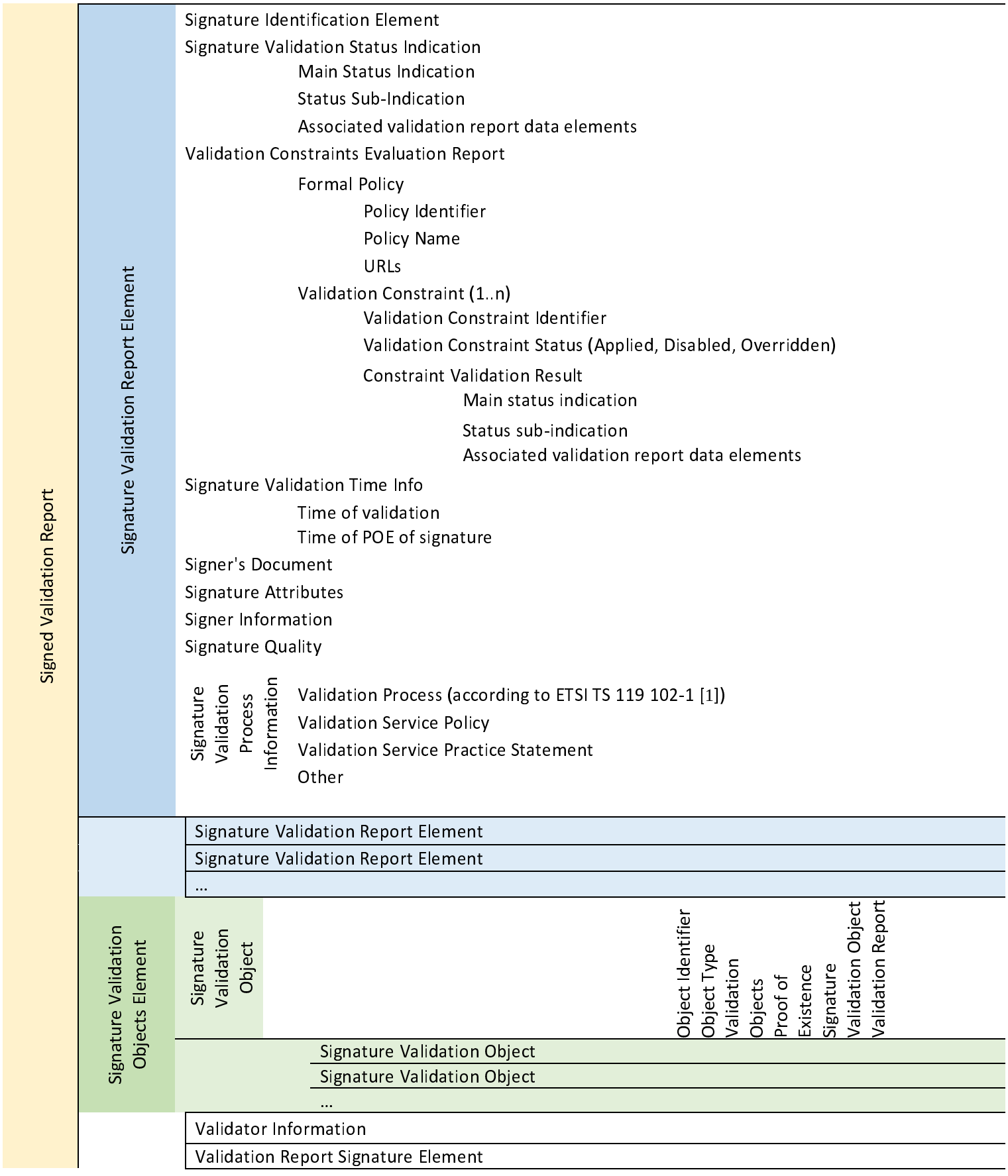

Figure 3: Validation Report Structure and Elements

ETSI defines in annex B a XML Schema file for the present document.

For every element specified below, a clause provides an excerpt of that schema that is relevant for that element for information. In case of discrepancies between such xml schema excerpts provided in the present document and the XML Schema files, the XML Schema files shall take precedence.

Conventional XML namespace prefixes are used in the present document:

- The prefix `vr:` (or no prefix) stands for the namespace for the present document.
- The prefix `ds:` stands for the W3C XML Signature namespace [2].
- The prefix `XAdES`: stands for the namespace defined in ETSI XML Advanced Electronic Signatures (XAdES) document [3].
- The prefix `tsl`: stands for the namespace defined in ETSI TS 119 612 [6].
- The prefix `xs`: stands for the XML schema namespace [10].

Table 1 shows the URI values of the XML namespaces and their corresponding prefixes used in the schema file and within the present document.

Table 1: Namespaces with prefixes

URI value of the XML Namespace	Prefix
http://uri.etsi.org/19102/v1.1.1#	vr
http://www.w3.org/2000/09/xmldsig#	ds
http://uri.etsi.org/01903/v1.3.2	XAdES
http://uri.etsi.org/02231/v2#	tsl
http://www.w3.org/2001/XMLSchema	xs

The following elements are used throughout the following clauses.

4.1.1.2 Validation Object Reference Element

4.1.1.2.1 General

Validation object reference elements are used within a validation report to reference another element within the report.

EXAMPLE: Signature validation objects or the Signature Identification Element can be such elements that are referenced.

4.1.1.2.2 XML

Validation object reference elements shall be type `VOReferenceType` that is defined as follows:

```
<xs:complexType name="VOReferenceType">
    <xs:attribute name="VOReference" type="xs:IDREF" use="required"/>
    <xs:sequence>
        <xs:any namespace="##any" processContents="lax" minOccurs="0"/>
    </sequence>
</xs:complexType>
```

4.1.1.3 Typed Data Type

4.1.1.3.1 General

A typed data type element is a generic data structure that can be used for representing any Type-Value tuple.

4.1.1.3.2 XML

A typed data type element shall be of type `TypedDataType` that is defined as follows:

```
<xs:complexType name="TypedDataType">
    <xs:sequence>
        <xs:element name="Type" type="xs:anyURI"/>
        <xs:element name="Value" type="xs:anyType"/>
    </xs:sequence>
</xs:complexType>
```

4.1.1.4 Signature Reference

4.1.1.4.1 General

A signature reference element references a specific electronic signature.

4.1.1.4.2 XML

A signature reference shall be of type `SignatureReferenceType` that is defined as follows:

```
<xs:complexType name="SignatureReferenceType">
    <xs:choice>
        <xs:sequence>
            <xs:element name="CanonicalizationMethod" type="xs:anyURI" minOccurs="0"/>
            <xs:element name="DigestMethod" type="xs:anyURI"/>
            <xs:element name="DigestValue" type="xs:base64Binary"/>
        </xs:sequence>
        <xs:element ref="vr:XAdESSignaturePtr"/>
        <xs:element name="PAdESFieldName" type="xs:string"/>
        <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:choice>
</xs:complexType>
<xs:element name="XAdESSignaturePtr" type="vr:XAdESSignaturePtrType"/>
<xs:complexType name="XAdESSignaturePtrType">
    <xs:sequence>
        <xs:element name="NsPrefixMapping" type="vr:NsPrefixMappingType"
            minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="WhichDocument" type="xs:IDREF" use="optional"/>
    <xs:attribute name="XPath" type="xs:string" use="optional"/>
    <xs:attribute name="SchemaRefs" type="xs:IDREFS" use="optional"/>
</xs:complexType>
<xs:complexType name="NsPrefixMappingType">
    <xs:sequence>
        <xs:element name="NamespaceURI" type="xs:anyURI"/>
        <xs:element name="NamespacePrefix" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
```

4.2 Validation-Report-Element

4.2.1 General

Presence: Mandatory

Description: This element is the wrapper for reports on the validation of one or more signatures.

Content: This element shall contain one or more signature-validation-report elements as specified in clause 4.3.
It also may contain:

- A signature validation objects element as specified in clause 4.4.
- Information on the entity validating the signature and creating the validation report as described in clause 4.5; and

- A validation-report-signature element as described in clause 4.6.

4.2.2 XML

The validation report element shall be contained in an element named `ValidationReport` of type `ValidationReportType` that is defined as follows:

```
    <xs:complexType name="ValidationReportType">
        <xs:sequence>
            <xs:element name="SignatureValidationReport" type="SignatureValidationReportType"
maxOccurs="unbounded"/>
            <xs:element name="SignatureValidationObjects" type="ValidationObjectListType"
                minOccurs="0"/>
            <xs:element name="SignatureValidator" type="SignatureValidatorType" minOccurs="0"/>
            <xs:element ref="ds:Signature" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
```

4.3 Signature-Validation-Report-Element

4.3.1 General

Presence: Mandatory

Description: This element represents the validation information for a single signature.

Content: This element shall contain a sequence of elements described in the clauses 4.3.3 to 4.3.12.

NOTE: This element is also used in the validation report of a signature validation object (see clause 4.4.8). The rules whether an element contained within this element is mandatory or optional can be different in this case.

This element may also contain any other information provided by the validation process.

4.3.2 XML

The signature validation report shall be contained in an element named `SignatureValidationReport` of type `SignatureValidationReportType` that is defined as follows:

```
    <xs:complexType name="SignatureValidationReportType">
        <xs:sequence>
            <xs:element name="SignatureIdentifier" type="SignatureIdentifierType" minOccurs="0"/>
            <xs:element name="ValidationStatus" type="ValidationStatusType"/>
            <xs:element name="ValidationConstraintsEvaluationReport"
                     type="ValidationConstraintsEvaluationReportType" minOccurs="0"/>
            <xs:element name="ValidationTimeInfo" type="ValidationTimeInfoType" minOccurs="0"/>
            <xs:element name="SignersDocument" type="SignersDocumentType" minOccurs="0"/>
            <xs:element name="SignatureAttributes" type="SignatureAttributesType "
                minOccurs="0"/>
            <xs:element name="SignerInformation" type="SignerInformationType" minOccurs="0"/>
            <xs:element name="SignatureQualityType" type="SignatureQualityType" minOccurs="0"/>
            <xs:element name="SignatureValidationProcessType"
                        type="SignatureValidationProcessType" minOccurs="0"/>
            <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

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

4.3.3 Signature Identification Element

4.3.3.1 Element Semantics

Presence: Conditional.
This element shall be present in the validation report of a signature.

This element may be present in a validation report of a signature validation object (see clause 4.4.8).

Description: This element identifies the signature that has been the scope of the validation.

Content: This element shall contain:

1) The DTBSR (see clause 4.2.8 in ETSI TS 119 102-1 [1]) together with an identifier of the hash algorithm used to calculate the hash.

2) An indication whether the DTBSF (see clause 4.2.7 in ETSI TS 119 102-1 [1]) or the DTBSR (see clause 4.2.8 in ETSI TS 119 102-1 [1]) has been processed by the SVA.

NOTE 1: This allows the report format defined in the present document to be used when a SVA has verified the cryptographic signature and the validity of the certificate(s) only without having seen the documents and any other elements of an AdES-Signature.

3) An indication whether the Signer's Document (SD) (see clause 4.2.3 in ETSI TS 119 102-1 [1]) or the Signer's Document representation (SDR) (see clause 4.2.4 in ETSI TS 119 102-1 [1]) has been processed by the SVA.

NOTE 2: This allows the report format defined in the present document to be used when a SVA has verified an AdES signature having processed the hash the Signer's Document only.

This element may also contain:

4) A unique identifier allowing this element to be referenced within the validation report.

5) The digital signature value.

6) An identifier provided by the DA.

7) One or more other elements, which help identifying a signature and the signature data in a unique manner.

4.3.3.2 XML representation

The Signature Identification Element shall be of type `SignatureIdentifierType.`

This element shall contain the DTBSR in an element of type `XAdES:DigestAlgAndValueType.`

The element `HashOnly` shall contain the value `true` when only the DTBSR has been processed by the SVA, otherwise it shall contain the value `false`.

The element `DocHashOnly` shall contain the value `true` when only the SD has been processed by the SVA, otherwise it shall contain the value `false`.

This element may also contain:

- A <`ds:SignatureValue`>-element to identify the signature by the digital signature value;
- A `DAIdentifier`-element containing an identifier provided by the DA; and
- An `xs:id` attribute as the unique identifier by which this element can be referenced;
- One or more `Other`-elements helping to identify the signature.

The set of child elements shall be chosen to identify the signature or validation data in an unambiguous manner.

```
    <xs:complexType name="SignatureIdentifierType">
        <xs:sequence>
            <xs:element name="DigestAlgAndValue" type="XAdES:DigestAlgAndValueType" minOccurs="0"/>
            <xs:element ref="ds:SignatureValue" minOccurs="0" />
            <xs:element name="HashOnly" type="xs:boolean"/>
            <xs:element name="DocHashOnly" type="xs:boolean"/>
            <xs:element name="DAIdentifier" type="xs:boolean"/>
            <xs:element name="Other" type="xs:anyType" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="id" type="xs:ID" use="required"/>
    </xs:complexType>
```

4.3.4 Signature Validation Status Indication

4.3.4.1 General

Presence: Mandatory.

Description: When present in the validation report of a signature, this element provides information on the status of the full validation of the signature in the context of a particular signature validation policy.
When present in a validation report of a signature validation object, this element provides information on the result of the validation of that object in the context of a particular signature validation policy that was selected for the validation of the signature.

Content: This element shall contain one main status indication element as defined in clause 4.3.4.2.

This element may contain one or more sub-indication elements as defined in clause 4.3.4.3.

NOTE: There can be more than one sub-indication element when the SVA needs to report multiple problems.

4.3.4.2 Main Status Indication Element

Presence: Mandatory.

Description: This element provides the main status indication.

Content: When present in the validation report of a signature, the following URIs shall be used to represent the main status indication:

- *TOTAL-PASSED:* urn:etsi:019102:mainindication:total-passed
- *TOTAL-FAILED* urn:etsi:019102:mainindication:total-failed
- *INDETERMINATE* urn:etsi:019102:mainindication:indeterminate

When present in an individual validation constraint report element (see clause 4.3.5.4) or a validation report of a signature validation object (see clause 4.4.8), the following URIs shall be used to represent the main status indication:

- *PASSED:* urn:etsi:019102:mainindication:passed
- *FAILED* urn:etsi:019102:mainindication:failed
- *INDETERMINATE* urn:etsi:019102:mainindication:indeterminate

The main status indication may be supported by associated validation report data as specified in tables 5 and 6 of ETSI TS 119 102-1 [1]. If present, such data shall be contained in associated validation data elements as specified in clauses 4.3.12.

4.3.4.3 Status Sub-Indication Element

Presence: Optional.

Description: This element provides a status sub-indication.

NOTE: When the main status indication is *TOTAL-FAILED* or *INDETERMINATE*, providing a sub-indication is essential to understand the reason for the result.

Content: The Status Sub-Indication element shall consist of:

1) A sub-indication that shall clearly identify the reason for the main status indication; and

2) Optional associated validation report data elements (see clause 4.3.12) supporting that sub-indication.

There may be more than one sub-indication element present.

A sub-indication may be supported by associated validation report data as specified in tables 5 and 6 of ETSI TS 119 102-1 [1]. If present, such data shall be contained in associated validation data elements as specified in clauses 4.3.12.

When the sub-indication corresponds to a sub-indication defined in ETSI TS 119 102-1 [1], the following URIs shall be used.

Subindication	URN
FORMAT_FAILURE	urn:etsi:019102:subindication:FORMAT_FAILURE
HASH_FAILURE	urn:etsi:019102:subindication:HASH_FAILURE
SIG_CRYPTO_FAILURE	urn:etsi:019102:subindication:SIG_CRYPTO_FAILURE
REVOKED	urn:etsi:019102:subindication:REVOKED
SIG_CONSTRAINTS_FAILURE	urn:etsi:019102:subindication:SIG_CONSTRAINTS_FAILURE
CHAIN_CONSTRAINTS_FAILURE	urn:etsi:019102:subindication:CHAIN_CONSTRAINTS_FAILURE
CERTIFICATE_CHAIN_GENERAL_FAILURE	urn:etsi:019102:subindication:CERTIFICATE_CHAIN_GENERAL_FAILURE
CRYPTO_CONSTRAINTS_FAILURE	urn:etsi:019102:subindication:CRYPTO_CONSTRAINTS_FAILURE
EXPIRED	urn:etsi:019102:subindication:EXPIRED
NOT_YET_VALID	urn:etsi:019102:subindication:NOT_YET_VALID
POLICY_PROCESSING_ERROR	urn:etsi:019102:subindication:POLICY_PROCESSING_ERROR
SIGNATURE_POLICY_NOT_AVAILABLE	urn:etsi:019102:subindication:SIGNATURE_POLICY_NOT_AVAILABLE
TIMESTAMP_ORDER_FAILURE	urn:etsi:019102:subindication:TIMESTAMP_ORDER_FAILURE
NO_SIGNING_CERTIFICATE_FOUND	urn:etsi:019102:subindication:NO_SIGNING_CERTIFICATE_FOUND
NO_CERTIFICATE_CHAIN_FOUND	urn:etsi:019102:subindication:NO_CERTIFICATE_CHAIN_FOUND
REVOKED_NO_POE	urn:etsi:019102: subindication:REVOKED_NO_POE
REVOKED_CA_NO_POE	urn:etsi:019102: subindication:REVOKED_CA_NO_POE
OUT_OF_BOUNDS_NO_POE	urn:etsi:019102:subindication:OUT_OF_BOUNDS_NO_POE
CRYPTO_CONSTRAINTS_FAILURE_NO_POE	urn:etsi:019102:subindication:CRYPTO_CONSTRAINTS_FAILURE_NO_POE
NO_POE	urn:etsi:019102:subindication:NO_POE
TRY_LATER	urn:etsi:019102:subindication:TRY_LATER
SIGNED_DATA_NOT_FOUND	urn:etsi:019102:subindication:SIGNED_DATA_NOT_FOUND

4.3.4.4 XML representation

The signature validation status indication shall be provided as an element named `SignatureValidationStatus` of type `ValidationStatusType`, as defined below.

The main status indication shall be expressed by the element `MainIndication` using the URIs defined in clause 4.3.4.2.

The sub-indication shall be expressed by the element `SubIndication` using the URIs defined in clause 4.3.4.3.

The associated validation data may be reported in `AssociatedValidationReportData` elements, see clause 4.3.12.

```
<xs:complexType name="ValidationStatusType">
    <xs:sequence>
        <xs:element name="MainIndication" type="xs:AnyURI"/>
        <xs:element name="SubIndication" type="xs:AnyURI" minOccurs="0" maxOccurs="Unbounded"/>
        <xs:element name="AssociatedValidationReportData" type="ValidationReportDataType"
                    minOccurs="0" maxOccurs="Unbounded" />
    </xs:sequence>
</xs:complexType>
```

4.3.5 Validation Constraints Evaluation Report

4.3.5.1 General

Presence: Conditional.
This element shall be present in the validation report of a signature.

This element may be present in a validation report of a signature validation object (see clause 4.4.8).

Description: This element specifies the set of validation constraints that have been driving the validation process, irrespective of the way the constraints have been defined (see ETSI TS 119 102-1 [1], clause 5.1.4.1).

Content: When a formal signature validation policy as defined in ETSI TS 119 172-1 [11] has been selected explicitly or implicitly by the DA, this element shall contain a reference to that formal signature validation policy specification in a *formal policy element* (see clause 4.3.5.3).

NOTE: The reference to the formal signature validation policy indicates that this policy has been driving the validation. Detailed information on the validation of the individual constraints this policy consists of can be reported additionally in validation constraint elements.

This element shall contain *individual validation constraint report elements* (see clause 4.3.5.4) reporting on validation constraints in that have been applied explicitly and implicitly by the SVA.

This element shall contain *individual validation constraint report elements* (see clause 4.3.5.4) reporting on validation constraints that a validation conformant to ETSI TS 119 102-1 [1] would require to be checked but have been disabled or being overridden by the validation policy in use.

When a formal signature validation policy provided by the DA was not applied or not applied completely by the SVA, the validation report shall contain *individual validation constraint report elements* (see clause 4.3.5.4) reporting on which validation constraints were applied and which ones have been ignored or overridden.

4.3.5.2 XML

Information on the validation constraints that were applied during validation shall be placed in an element named `ValidationConstraintsEvaluationReport` of type `ValidationConstraintsEvaluationReportType`, defined as follows:

```
<complexType name="ValidationConstraintsEvaluationReportType">
    <xs:sequence>
        <xs:element name="SignatureValidationPolicyType" minOccurs="0" />
        <xs:element name="ValidationConstraint" type="IndividualValidationConstraintReportType"
            minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
</complexType>
```

It may contain an element of type `SignatureValidationPolicyType` as defined in clause 4.3.5.3.2 and one or more elements of type `IndividualValidationConstraintReportType` as defined in clause 4.3.5.4.2.

4.3.5.3 Formal Policy Element

4.3.5.3.1 General

Presence: Conditional.

This element shall be present in the validation report of a signature when a formal signature validation policy as defined in ETSI TS 119 172-1 [11] has been selected explicitly or implicitly by the DA.

In all other cases, this element may be present.

Description: This element defines a formal signature validation policy that has been driving the validation process.

Content: This element shall contain a signature validation policy identifier that is capable of uniquely identifying the signature validation policy defining the set of constraints that have been applied during validation.

This element may also contain the following additional information:

1) A signature policy name;

2) A URL where the formal policy specification can be retrieved;

3) A URL where a human readable policy equivalent to the applied formal policy can be retrieved;

4) A reference to an object in the Signature Validation Objects element (see clause 4.1.1.2). The object referenced shall contain the formal signature validation policy specification.

4.3.5.3.2 XML

This element shall be encoded in an element named `SignatureValidationPolicy` of type `SignatureValidationPolicyType`, where:

- The signature validation policy identifier shall be contained in an element `SignaturePolicyId` of Type `XAdES:SignaturePolicyIdentifierType`;
- When present, the signature policy name shall be contained in an element named `PolicyName` and of type `xs:string`;
- When present, the URL of the formal policy specification shall be contained in an element named `FormalPolicyURI` of type `xs:AnyURI`;
- When present, the URL of the human readable policy shall be contained in an element named `ReadablePolicyURI` of type `xs:AnyURI`;
- When present, the reference to an object on the Signature Validation Objects element shall be contained in an element named `FormalPolicyObject` of type `VOReferenceType`.

```
<xs:complexType name="SignatureValidationPolicyType">
    <xs:sequence>
        <xs:element name="SignaturePolicyId" type="XAdES:SignaturePolicyIdentifierType"
                    minOccurs="0"/>
        <xs:element name="PolicyName" type="xs:string" minOccurs="0"/>
        <xs:element name="FormalPolicyURI" type="xs:anyURI" minOccurs="0"/>
        <xs:element name="ReadablePolicyURI" type="xs:anyURI" minOccurs="0"/>
        <xs:element name="FormalPolicyObject" type="vr:VOReferenceType" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

4.3.5.4 Individual Validation Constraint Report Element

4.3.5.4.1 General

Presence: Optional.

Description: This element shall indicate an individual signature validation constraint that has been applied during validation.

Content: This element shall contain the following information:

1) A validation constraint identifier that is capable of uniquely identifying a validation constraint;

2) Whether the constraint was applied, disabled or overridden by another constraint, and if the latter, by which one;

When the validation of the constraint has not been disabled or overridden:

3) The validation result for the constraint;

The validation result shall be represented by a main status indication (PASSED, FAILED, INDETERMINATE). It may be supported by a sub-indication and additional associated validation report data elements (see clause 4.3.12).

In addition, this element may also contain:

4) Any parameters the validation constraint requires;

5) Indications for steps to be taken to potentially get a determinate result, when the main status indication is INDETERMINATE.

EXAMPLE: Possible parameters are a set of trust anchors or how revocation checking is to be done.

4.3.5.4.2 XML

The validation report for a single validation constraint shall be contained in an element of type `IndividualValidationConstraintType` defined as follows:

```
<xs:complexType name="IndividualValidationConstraintReportType">
    <xs:sequence>
        <xs:element name="ValidationConstraintIdentifier" type="xs:anyURI"/>
        <xs:element name="ValidationConstraintParameter" type="vr:TypedDataType"
            minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="ConstraintStatus" type="vr:ConstraintStatusType"/>
        <xs:element name="ValidationStatus" type="vr:ValidationStatusType" minOccurs="0"/>
        <xs:element name="Indications" type="xs:anyType" minOccurs="0"/>
</xs:sequence>
```

The validation constraint identifier that is capable of uniquely identifying a validation constraint shall be contained in an element named `ValidationConstraintIdentifier` and of type `xs:anyURI`.

The information whether the constraint was applied, disabled or overridden by another constraint, and if so, by which one, shall be contained in an element named `ConstraintStatus` of type `ConstraintStatusType`. This type is defined as follows:

```
<xs:complexType name="ConstraintStatusType">
    <xs:sequence>
        <xs:element name="Status" type="xs:anyURI"/>
        <xs:element name="OverriddenBy" type="xs:anyURI" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

The `Status`-element shall contain one of the following URIs:

- When the constraint has been applied: urn:etsi:019102:constraintStatus:applied;
- When the constraint has been disabled: urn:etsi:019102:constraintStatus:disabled;
- When the constraint has been overridden by another constraint: urn:etsi:019102:constraintStatus:overridden. In this case, the OverriddenBy element shall indicate the other constraint.

Whenever the `Status`-element of `ConstraintStatus` contains the value `urn:etsi:019102:constraintStatus:applied,` the validation result for the constraint shall be contained in an element named `ValidationStatus` and be of type `ValidationStatusType`.

When present, parameters the validation constraints requires shall be contained in an element named `ValidationConstraintParameter` of type `TypedDataType`.

When present, indications for steps to be taken to potentially get a determinate result, when the main status indication is INDETERMINATE shall be contained in an element named `Indications` of type `xs:anyType`.

4.3.6 Signature Validation Time Info

4.3.6.1 General

Presence: Conditional.
This element shall be present in the validation report of a signature.

This element may be present in a validation report of a signature validation object (see clause 4.4.8).

Description: This element provides time related information on the validation.

Content: This element shall contain:

1) The date and time the validation was performed; and

2) The date and time for which a POE of the signature has been identified and the validation status has been determined.

This element may also contain information on the source of the POE and, when the POE was derived by the SVA, an identifier referencing the signature validation object that was essential for that proof.

Date and time information shall be provided in UTC.

NOTE: The second value is the current time for Basic Signature validation; it can be either the current time or a point in time in the past when validating Signatures with Time, Signatures with Long-Term-Validation Material or Signatures providing Long Term Availability and Integrity of Validation Material.

4.3.6.2 XML

The signature validation time info shall be contained in an element of type `ValidationTimeInfo` of type `ValidationTimeInfoType` which is defined as follows:

```
<xs:complexType name="ValidationTimeInfoType">
    <xs:sequence>
        <xs:element name="ValidationTime" type="xs:dateTime"/>
        <xs:element name="BestSignatureTime" type="vr:POEType"/>
    </xs:sequence>
</xs:complexType>
```

The date and time the validation was performed shall be contained in the element `ValidationTime`.

The date and time for which a POE of the signature has been identified and the validation status has been determined shall be contained in the element BestSignatureTime that shall be of type `POEType` (see clause 4.4.6).

4.3.7 Signer's Document Element

4.3.7.1 General

Presence: Conditional.
This element shall be present in the validation report of a signature.

This element may be present in a validation report of a signature validation object (see clause 4.4.8).

Description: This element identifies the document that has been covered by the signature.

Content: This element shall contain the Signer's document representation (SDR).

This element may also contain a reference to a signature validation object within the Signature Validation Objects - Element (see clause 4.4) whenever the SD has been provided by the DA to the SVA. When present, the validation object shall contain the SD or a URI allowing to retrieve the SD.

4.3.7.2 XML

The signer's document element shall be represented as an element named `SignersDocument` of type `SignersDocumentType`.

This element shall contain the SDR in an element of type `XAdES:DigestAlgAndValueType`.

This element may also contain the reference to the signer's document in an element of type `vr:VOReferenceType`.

```
<xs:complexType name="SignersDocumentType">
    <xs:sequence>
        <xs:element name="DigestAlgAndValue"
            type="XAdES:DigestAlgAndValueType"/>
        <xs:element name="SignersDocumentRef" type="VOReferenceType" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

4.3.8 Signature Attribute Element

4.3.8.1 General

Presence: Conditional.
This element shall be present whenever the signature contains signature attributes.

Description: This element provides the signature attributes that were present in the validated signature.

Content: This element shall consist of a sequence with one instance per attribute contained in the signature. Each element of that sequence shall contain:

1) The type of the attribute.

2) Whether the attribute was a signed or an unsigned attribute.

It also may contain:

3) Attribute dependant information extracted from the attribute. Annex B specifies such information for attributes that are defined for CAdES [i.1], PAdES [i.3] and XAdES [4].

4) One or more references to signature validation objects within the Signature Validation Objects - Element (see clause 4.4).

4.3.8.2 XML

The signature attributes element shall be contained in an element named `SignatureAttributes` containing a sequence of elements which are extensions of `AttributeBaseType`. Each of these elements shall contain a boolean XML-Attribute Signed which indicates, whether the attribute was a signed or unsigned attribute.

Annex B specifies how attributes that are defined for CAdES [i.1], PAdES [i.3] and XAdES [4] signatures are to be represented in XML.

```
<xs:complexType name="SignatureAttributesType">
    <xs:sequence>
        <xs:choice maxOccurs="unbounded">
            <!—elements are defined in Annex B -->
        </xs:choice>
```

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

    <xs:complexType name="AttributeBaseType">
        <xs:attribute name="Signed" type="xs:boolean" use="optional"/>
        <xs:sequence>
            <xs:element name="AttributeObject" type="vr:VOReferenceType"
                    minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
```

4.3.9 Signer Information Element

4.3.9.1 General

Presence: Conditional.
When a signing certificate was identified, this element shall be present in the validation report of a signature.

Otherwise, this element may be present.

Description: This element provides information on the signer.

Content: This element shall contain a reference to an object in the Signature Validation Objects element (see clause 4.4). The object referenced shall be the certificate that has been identified as the signer's certificate and that contains the unique set of data representing the signer.

This element may also contain a human readable representation of the signer.

EXAMPLE: Examples are the distinguished name or the subject alternate name contained in the signer's certificate.

When a pseudonym has been used at the time of signing, this element shall contain an indication that a pseudonym has been used.

4.3.9.2 XML

The signer information shall be contained in an element named `SignerInformation` and of type `vr:SignerInformationType`.

This element shall contain the reference to the signer's certificate in an element of type `vr:VOReferenceType`.

It may contain a string representation identifying the signer and optional other information about the signer.

When a pseudonym is used, the element shall contain the `Pseudonym` attribute indicating this.

```
    <xs:complexType name="SignerInformationType">
        <xs:attribute name="Pseudonym" type="boolean" use="optional" />
        <xs:sequence>
            <xs:element name="SignerCertificate" type="VOReferenceType" />
            <xs:element name="Signer" type="string" minOccurs="0"/>
            <xs:any namespace="##other" minOccur="0"/>
        </xs:sequence>
    </xs:complexType>
```

4.3.10 Signature Quality Element

4.3.10.1 General

Presence: Optional.

Description: This element contains information supporting the quality of the signature.

EXAMPLE: Qualified electronic signature, advanced electronic signature supported by a qualified certificate.

Content: This element shall contain one or more URN indicating the quality of the signature.

NOTE: It is out of scope for the present document to define the URNs for signature quality.

4.3.10.2 XML

The signature quality information shall be contained in an element named `SignatureQuality` and of type `vr:SignatureQualityType`.

```
<xs:complexType name="SignatureQualityType">
    <xs:sequence>
        <xs:element name="SignatureQalityInformation" type="xs:anyURI" minOccurs="0"
            maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

4.3.11 Signature Validation Process Information Element

4.3.11.1 General

Presence: Optional.

Description: This element provides information on the signature validation process performed.

Content: This element shall contain one or more of:

1) A URI indicating the validation process (see ETSI TS 119 102-1 [1], clauses 5.3, 5.5, 5.6.3) that has been used for validation. This URI shall have one of the following values:

   - `urn:etsi:019102:validationprocess:Basic` when the SVA performed the Validation Process for Basic Signatures as specified in ETSI TS 119 102-1 [1], clause 5.3.
   - `urn:etsi:019102:validationprocess:LTVM` when the SVA performed the Validation Process for Signatures with Time and Signatures with LongTerm-Validation Material as specified in ETSI TS 119 102-1 [1], clause 5.5.
   - `urn:etsi:019102:validationprocess:LTA` when the SVA performed the Validation process for Signatures providing Long Term Availability and Integrity of Validation Material as specified in ETSI TS 119 102-1 [1], clause 5.6.

   Any other `URI` indicating the validation process when none of these processes has been applied:

2) A URI identifying the validation service policy, when applicable;

3) A URI identifying the validation service practice statement, when applicable;

4) Other information provided by the validation process.

4.3.11.1 XML

This element shall be named `SignatureValidationProcessInfo` and be of type `SignatureValidationProcessInfoType`. It is defined as follows:

```
<xs:complexType name="SignatureValidationProcessType">
    <xs:sequence>
        <xs:element name="SignatureValidationProcessID" type="anyURI" minOccurs="0"/>
        <xs:element name="SignatureValidationServicePolicy" type="anyURI" minOccurs="0"/>
        <xs:element name="SignatureValidationPracticeStatement" type="anyURI" minOccurs="0"/>
        <xs:any namespace="##other" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

4.3.12 Associated Validation Report Data Element

4.3.12.1 General

Presence: Optional.

Description: This element contains additional information on the validation of the signature or a signature validation constraint.

Content: This element shall contain one or more of the elements described in the clauses 4.3.12.3 to 4.3.12.8.

4.3.12.2 XML

Associated Validation Report Data shall be provided in an element named `AssociatedValidationReportData` of type `ValidationReportDataType` that is defined as follows:

```
<xs:complexType name="ValidationReportDataType">
    <xs:sequence>

        <xs:element name="TrustAnchor" type="vr:VOReferenceType" minOccurs="0"/>
        <xs:element name="CertificateChain" type="vr:CertificateChainType" minOccurs="0"/>
        <xs:element name="SignedDataObjects" type="vr:SignedDataObjectsType" minOccurs="0"/>
        <xs:element name="RevocationStatusInformation" type="vr:RevocationStatusInformationType"
                    minOccurs="0"/>
        <xs:element name="CryptoInformation" type="vr:CryptoInformationType" minOccurs="0"/>
        <xs:element name="AdditionalValidationReportData"
                    type="vr:AdditionalValidationReportDataType" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

4.3.12.3 Trust Anchor Element

4.3.12.3.1 General

Presence: Optional.

Description: This element identifies the public key that has been used as the trust anchor in the validation process.

Content: This element shall contain an identifier referencing an object in the Signature Validation Objects element (see clause 4.4) that contains a certificate for the public key of the trust anchor.

It may also contain additional information provided by the validation process.

4.3.12.3.2 XML

This element shall have the name `TrustAnchor` and be of type `VOReferenceType` and shall contain the identifier of the object in the Signature Validation Objects element that has been used as the trust anchor in the validation process. The object referenced shall be a certificate or a public key.

4.3.12.4 Certificate Chain Element

4.3.12.4.1 General

Presence: Optional.

Description: This element identifies the certificate chain.

Content: This element shall contain a list of identifiers referencing objects in the Signature Validation Objects element (see clause 4.4). This list shall contain the identifiers for the signing certificate (clause 4.3.9) as the first element and the trust anchor (clause 4.3.12.3) as the last element. The certificates referenced by this list shall be the certificate chain used in the validation process.

This element may also contain additional information provided by the validation process.

4.3.12.4.2 XML

This element shall have the name `CertificateChain` and shall be a sequence of elements of type `VOReferenceType` (see clause 4.1.1.2). The first element of the sequence shall have the name `SigningCertificate` and contain a reference to the signing certificate. The last element of the list shall have the name `TrustAnchor` and contain a reference to the trust anchor. All other elements shall have the name `IntermediateCertificate` and contain a reference to the corresponding intermediate certificate.

```
<xs:complexType name="CertificateChain">
    <xs:sequence>
        <xs:element name="SigningCertificate" type="VOReferenceType"/>
        <xs:element name="IntermediateCertificate" type="VOReferenceType" minOccurs="0"
            maxOccurs="unbounded"/>
        <xs:element name="TrustAnchor" type="VOReferenceType" minOccurs="0"/>
        <xs:any namespace="##any" processContents="lax" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

4.3.12.5 Signed Data Objects Element

4.3.12.5.1 General

Presence: Optional.

Description: This element relates a validation status sub-indication or a validation constraint sub-indication to the data objects that caused that sub-indication.

Content: This element shall contain a list of references to signed data objects in the Signature Validation Objects element (see clause 4.4). This list shall not be an empty list.

NOTE: This list can contain one element only.

EXAMPLE: In case of a TIMESTAMP_ORDER_FAILURE, this element contains a list of references to the timestamps that caused that failure.

4.3.12.5.2 XML

This element shall be of type `SignedDataObjectsType` and shall contain a list of elements of type `VOReferenceType` uniquely identifying signed data objects in the Signature Validation Objects element.

```
<xs:complexType name="SignedDataObjectsType">
    <xs:sequence>
        <xs:element name="SignedDataObject" type="vr:VOReferenceType"
            maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

4.3.12.6 Revocation Status Information Element

4.3.12.6.1 General

Presence: Conditional.
This element shall be present when a certificate has been found to be revoked.

Description: When a certificate has been found to be revoked, this element contains information on the revocation.

Content: This element shall contain:

1) An identifier referencing a certificate in the Signature Validation Objects element (see clause 4.4);

2) The time of revocation.

It may also contain:

3) A reason for the revocation;

4) An identifier referencing a CRL or OCSP response in the Signature Validation Objects element that has been used for determining that revocation status;

5) Additional information provided by the validation process.

4.3.12.6.2 XML

This element shall be of type `RevocationStatusInformationType` that is defined as follows:

```
<xs:complexType name="RevocationStatusInformationType">
    <xs:sequence>
        <xs:element name="ValidationObject" type="VOReferenceType"/>
        <xs:element name="RevocationTime" type="xs:dateTime"/>
        <xs:element name="RevocationReason" type="anyURI" minOccurs="0"/>
        <xs:element name="RevocationObject" type="VOReferenceType" minOccurs="0"/>
        <xs:any namespace="##any" processContents="lax" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

The element `ValidationObject` shall reference a certificate in the Signature Validation Objects element.

The element `RevocationTime` shall contain the date and time of the revocation in UTC.

The element `RevocationReason` shall contain the reason for the revocation. When present, one of the following URIs shall be used:

```
urn:etsi:019102:revocationReason:unspecified
urn:etsi:019102:revocationReason:keyCompromise
urn:etsi:019102:revocationReason:cACompromise
urn:etsi:019102:revocationReason:affiliationChanged
urn:etsi:019102:revocationReason:superseded
urn:etsi:019102:revocationReason:cessationOfOperation
urn:etsi:019102:revocationReason:certificateHold
urn:etsi:019102:revocationReason:privilegeWithdrawn
```

When present, the element `RevocationObject` shall contain an identifier referencing a CRL or OCSP response in the Signature Validation Objects element that has been used for determining that revocation status.

4.3.12.7 Crypto Information Element

4.3.12.7.1 General

Presence: Conditional.
This element shall be present when the main status indication is INDETERMINATE and the sub-indication is CRYPTO_CONSTRAINTS_FAILURE. In all other cases, this element may be present.

Description: When the validation process determines that the cryptographic algorithm is no longer reliable, this element contains details on the algorithm.

Content: This element shall contain:

1) An identifier referencing an object in the Signature Validation Objects element (see clause 4.4) or the Signature Identification Element (see clause 4.3.3);

2) A URI referencing a cryptographic algorithm that has been used when producing the object or the signature; and

3) An element specifying whether the algorithm and the algorithm-parameters were considered secure or insecure.

Algorithms that are listed in ETSI TS 119 312 [7] shall be represented by URIs defined in the same place.

This element may additionally contain:

4) Parameters that have been used when applying the algorithm;

5) Time information up to which the algorithm or algorithm-parameters were considered secure;

6) Additional information provided by the validation process

NOTE: This element can also be used when reporting on the used algorithms even when they are not expired.

4.3.12.7.2 XML

This element shall be of type `CryptoInformationType` that is defined as follows:

```
<xs:complexType name="CryptoInformationType">
    <xs:sequence>
        <xs:element name="ValidationObject" type="VOReferenceType"/>
        <xs:element name="Algorithm" type="xs:anyURI"/>
        <xs:element name="SecureAlgorithm" type="xs:boolean">
        <xs:element name="AlgorithmParameters" type="TypedDataType" minOccurs="0"/>
        <xs:element name="NotAfter" type="xs:dateTime" minOccurs="0"/>
        <xs:any namespace="##any" processContents="lax" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

The element `ValidationObjectId` shall contain an identifier referencing a signed object in the Signature Validation Objects element or a Signature Identification Element.

The element `Algorithm` shall contain a URI that identifies the algorithm.

When present, the element `AlgorithmParameters` shall specify algorithm-specific parameters that have been used.

When present, the element `NotAfter` shall contain the time when the algorithm or parameter was or will no longer be considered secure.

4.3.12.8 Additional Validation Report Data

4.3.12.8.1 General

Presence: Optional.

Description: This element can contain any additional information that the validation process provides.

Content: When present, this element shall contain one or more of the following:

1) An identifier identifying the type of additional information present;

2) The additional information.

4.3.12.8.2 XML

This element shall be of type `AdditionalValidationReportDataType` and contain one or more of the following tuple:

- An identifier identifying the type of additional information present
- The additional information

and is defined as follows:

```
<xs:complexType name="AdditionalValidationReportDataType">
    <xs:sequence>
        <xs:element name="ReportData" type="TypedDataType" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

4.4 Signature Validation Objects

4.4.1 General

Presence: Optional.

Description: This element is the container for validation objects used during validation.

NOTE: This avoids duplication of validation objects, e.g. CRLs, when the validation report contains the report on more than one signature or validation object.

Content: When present, this element shall contain a sequence of signature validation object elements representing the set of validation objects that have been used in the validation process together with their validation report, when applicable.

EXAMPLE: Signer's Document, Trusted Lists, revocation information (CRLs, OCSP-responses) or Evidence Records.

Each signature validation object element in this list shall have the following properties described in the clauses below:

- An identifier uniquely referencing this validation object within the validation report;
- The type of the object;
- The object itself or a reference to the object.

In addition, the following information about the signature validation object may be present:

- Information on a proof for the earliest time of the existence of the object;
- Information on objects the validation object provides proofs of existence for;
- A validation report on the validation of the object.

4.4.2 XML

The signature validation objects shall be placed in an element named `SignatureValidationObjects` of type `ValidationObjectListType`. Each element in this list shall be named `ValidationObject` and be of type `ValidationObjectType`.

```
<xs:complexType name="ValidationObjectListType">
    <xs:sequence>
        <xs:element name="ValidationObject" type="ValidationObjectType" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="ValidationObjectType">
    <xs:attribute name="id" type="xs:ID" use="required"/>
    <xs:sequence>
        <xs:element name="ObjectType" type="xs:anyURI"/>
        <xs:element name="ValidationObject" type="ValidationObjectRepresentationType"/>
        <xs:element name="POE" type="POEType" minOccurs="0"/>
        <xs:element name="POEProvisioning" type="POEProvisioningType" minOccurs="0"/>
        <xs:element name="ValidationReport" type="SignatureValidationReportType"/>
    </xs:sequence>
</xs:complexType>
```

To specify the type of validation object in the `ObjectType` element, one of the following URIs shall be used:

```
urn:etsi:019102:validationObject:certificate
urn:etsi:019102:validationObject:CRL
urn:etsi:019102:validationObject:OCSPResponse
urn:etsi:019102:validationObject:timestamp
urn:etsi:019102:validationObject:evidencerecord
urn:etsi:019102:validationObject:publicKey
urn:etsi:019102:validationObject:signedData
urn:etsi:019102:validationObject:other
```

The validation report of the validation object shall be of type `SignatureValidationReportType`.

4.4.3 Object Identifier

Presence: Mandatory.

Description: This element allows to uniquely reference this validation object within the validation report.

Content: This element shall contain an identifier that is unique within the validation report.

XML: This element shall be an attribute of type `xs:ID`.

4.4.4 Object Type

Presence: Mandatory.

Description: This element identifies the type of the validation object.

Content: This element shall contain a URI uniquely able to identify the type of the object.

XML: This element shall be an element named `ObjectType` of type `xs:anyURI`.

4.4.5 Validation Object

4.4.5.1 General

Presence: Mandatory.

Description: This element contains or references the validation object.

Content: This element shall contain one or more of the following:

1) The object itself;
2) A base64-encoded version of the object;
3) A cryptographic hash of the object; or
4) A URI where the object can be retrieved.

4.4.5.2 XML

Information on the validation object shall be placed in an element named `ValidationObject` of type `ValidationObjectRepresentationType`, defined as follows:

```
<xs:complexType name="ValidationObjectRepresentationType">
    <xs:choice>
        <xs:element name="direct" type="xs:anyType" minOccors="0"/>
        <xs:element name="base64" type="xs:base64Binary" minOccors="0"/>
        <xs:element name="DigestAlgAndValue" type="XAdES:DigestAlgAndValueType" minOccurs="0"/>
        <xs:element name="URI" type="xs:anyURI" minOccors="0"/>
    </xs:choice>
</xs:complexType>
```

4.4.6 Proof of Existence (POE)

4.4.6.1 General

Presence: Optional.

Description: This element contains information on a proof for the earliest time of the existence of the object.

Content: This element shall contain the information on the POE providing the earliest time for the existence of the object.

This property shall contain:

1) The time value for that proof in UTC;

2) An indication whether the POE has been:

   - derived during validation,
   - provided to the SVA as an input, or
   - derived by the policy.

EXAMPLE 1: A policy can require using the claimed signing time as a POE for the signature.

This element may also contain:

3) An identifier referencing the signature validation object that was essential for that proof.

EXAMPLE 2: Evidence records or time stamps can be such signature validation objects essential for that proof.

4.4.6.2 XML

```
<xs:complexType name="POEType">
    <xs:sequence>
            <xs:element name="POETime" type="xs:dateTime"/>
            <xs:element name="TypeOfProof" type="xs:anyURI"/>
            <xs:element name="POEObject" type="VOReferenceType" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

The element `POETime` shall contain the time value for the proof of existence.

The element `TypeOfProof` shall contain a URI indicating the origin of the POE. This element shall have one of the following values:

- `urn:etsi:019102:poetype:validation` when the POE has been derived during validation;
- `urn:etsi:019102:poetype:provided` when the POE has been provided to the SVA as an input;
- `urn:etsi:019102:poetype:policy` when the POE has been derived by the policy.

When present, the element `POEObject` shall contain the reference to the signature validation object that was essential for that proof.

4.4.7 POE Provisioning

4.4.7.1 General

Presence: Optional.

Description: When a validation object provides proofs of existence for other objects, this property provides information on these objects.

Content: This element shall contain:

1) The time value for that proof in UTC;

2) A list of references to the signature or to signature validation objects within the signature validation report that are covered by that proof.

NOTE: This element can be used to present the relationship between timestamps and timestamped data.

EXAMPLE: Time-stamps and evidence records can provide proofs of existence.

4.4.7.2 XML

```
<xs:complexType name="POEProvisioningType">
    <xs:sequence>
            <xs:element name="POETime" type="xs:dateTime"/>
            <xs:element name="ValidationObject" type="VOReferenceType" minOccurs="0"
                    maxOccurs="unbounded"/>
            <xs:element name="SignatureReference" type="vr:SignatureReferenceType"
                    minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

4.4.8 Validation Object validation report

Presence: Optional.

This element may be present whenever the signature validation object is a signed object and the signature has been validated during the overall validation.

Description: This element contains a validation report for the signature validation object.

Content: This element shall contain a validation report on the validation of the signature validation object. The report shall conform to the present document. Any validation object that was used in validation of this object shall be included in the Signature Validation Object element of the main validation report.

NOTE: The signature on the main validation report protects the validation report for a validation object.

4.5 Validator Information

4.5.1 General

Presence: Optional.

Description: This element identifies the entity validating the signature and creating the validation report.

Content: This element shall contain the digital identity of the validation service as specified in clause 5.5.3 of ETSI TS 119 612 [6].

This element may contain other information about the TSP as specified in clause 5.4 of ETSI TS 119 612 [6] as well as any additional information that can be used to identify the validator.

4.5.2 XML

The Validator Information Element shall be an element of type `SignatureValidatorType` as:

```
    <xs:complexType name="SignatureValidatorType">
        <xs:sequence>
            <xs:element name="DigitalId" type="tsl:DigitalIdentityType"
                maxOccurs="unbounded"/>
            <xs:element name="TSPInformation" type="tsl:TSPInformationType" minOccurs="0" />
            <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    <xs:/complexType>
```

4.6 Validation Report Signature

Presence: Optional.

Description: This element contains the validation report signature.

Content: When present, this element shall contain the signature over the signature validation report and shall be created by the validation service that performed the validation and created the validation report.

EXAMPLE: The following `SignedInfo`-element is an example of a signature over a report:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
  <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
  <Reference URI="">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>X2eAfTx6w22nZUfeKwIZ1oT33FH2LoBvI2xW4+MW/2s=</DigestValue>
  </Reference>
 </SignedInfo>
 …
</Signature>
```

Annex A (normative): Signature attribute representation

A.1 SignatureAttributesType

A.1.1 General

The `SignatureAttributesType` allows reporting on different signed and unsigned attributes. For those attributes defined in CAdES (ETSI EN 319 122-1 [i.1]), XAdES (ETSI EN 319 132-1 [4]) and PAdES (ETSI EN 319 142-1 [i.3]) this annex shows how they shall be represented.

When the signature reported in the validation report is neither XAdES nor CAdES nor PAdES, but still has one or more attributes defined in the aforementioned standards, the validation report may contain the components defined in the present annex, which allow to report on the aforementioned attributes.

EXAMPLE: A XML signature with a combination of XAdES qualifying property that does not correspond to any of the XAdES signature levels.

It is out of the scope of the present document how to report on attributes that have been specified neither in CAdES nor in PAdES nor in XAdES.

Any element not defined in this annex, which is used to report on an attribute within the `SignatureAttributesType`, shall be an extension of `BaseAttributeType`.

A.1.2 XML

The signed and unsigned attributes are reported on using the `SignatureAttributes` element, which is of type `SignatureAttributesType`.

The different choices allow to report on each of the attributes defined in CAdES (ETSI EN 319 122-1 [i.1]), XAdES (ETSI EN 319 132-1 [4]) and PAdES (ETSI EN 319 142-1 [i.3]).

```
    <xs:complexType name="SignatureAttributesType">
        <xs:sequence>
            <xs:choice maxOccurs="unbounded">
                <xs:element name="SigningTime" type="vr:SASigningTimeType"/>
                <xs:element name="SigningCertificate" type="vr:SACertIDListType"/>
                <xs:element name="DataObjectFormat" type="vr:SADataObjectFormatType"/>
                <xs:element name="CommitmentTypeIndication"
                            type="vr:SACommitmentTypeIndicationType"/>
                <xs:element name="AllDataObjectsTimeStamp" type="vr:SATimestampType"/>
                <xs:element name="IndividualDataObjectsTimeStamp" type="vr:SATimestampType"/>
                <xs:element name="SignaturePolicyIdentifier"
                            type="vr:SASignaturePolicyIdentifierType"/>
                <xs:element name="SignatureProductionPlace"
                            type="vr:SASignatureProductionPlaceType"/>
                <xs:element name="SignerRole" type="vr:SASignerRoleType"/>
                <xs:element name="CounterSignature" type="vr:SACounterSignatureType"/>
                <xs:element name="SignatureTimeStamp" type="vr:SATimestampType"/>
                <xs:element name="CompleteCertificateRefs" type="vr:SACertIDListType"/>
                <xs:element name="CompleteRevocationRefs" type="vr:SARevIDListType"/>
                <xs:element name="AttributeCertificateRefs" type="vr:SACertIDListType"/>
                <xs:element name="AttributeRevocationRefs" type="vr:SARevIDListType"/>
                <xs:element name="SigAndRefsTimeStamp" type="vr:SATimestampType"/>
                <xs:element name="RefsOnlyTimeStamp" type="vr:AttributeBaseType"/>
                <xs:element name="CertificateValues" type="vr:AttributeBaseType"/>
                <xs:element name="RevocationValues" type="vr:AttributeBaseType"/>
                <xs:element name="AttrAuthoritiesCertValues" type="vr:AttributeBaseType "/>
                <xs:element name="AttributeRevocationValues" type="vr:AttributeBaseType"/>
                <xs:element name="TimeStampValidationData" type="vr:AttributeBaseType"/>
                <xs:element name="ArchiveTimeStamp" type="vr:SATimestampType"/>
                <xs:element name="RenewedDigests" type="vr:SAListOfIntegers"/>
                <xs:element name="MessageDigest" type="vr:SAMessageDigestType"/>
                <xs:element name="DSS" type="vr:SADSSType"/>
```

```
            <xs:element name="VRI" type="vr:SAVRIType"/>
            <xs:element name="DocTimeStamp" type="vr:SATimestampType"/>
            <xs:element name="Reason" type="vr:SAReasonType"/>
            <xs:element name="Name" type="vr:SANameType"/>
            <xs:element name="ContactInfo" type="vr:SAContactInfoType"/>
            <xs:element name="SubFilter" type="vr:SASubFilterType"/>
            <xs:element name="ByteRange" type="vr:SAListOfIntegers"/>
            <xs:element name="Filter" type="vr:SAFilterType"/>
            <xs:any namespace="##other"/>
        </xs:choice>
    </xs:sequence>
</xs:complexType>
```

All the children of `SignatureAttributes` instances shall be instances of types derived from `AttributeBaseType`.

Most of the children of `SignatureAttributes` instances have been given the names of the qualifying properties of XAdES. In order to avoid ambiguities, the present annex will use the following convention:

- For a reference to an actual XAdES qualifying property it will use the prefix "`XAdES:`" preceding the local name of that property.
- For a reference to one of the children of `SignatureAttributes` instances defined in the present annex it will use the name without any prefix.

EXAMPLE: `XAdES:SigningCertificate` refers to the actual XAdES qualifying property, while `SigningCertificate` refers to the `SigningCertificate` child element of `SignatureAttributes` instances.

Depending on the qualifying property being reported, the namespace referenced by the `XAdES` prefix may be the one with the URI `http://uri.etsi.org/01903/v1.3.2#`, or `http://uri.etsi.org/01903/v1.4.1#`.

A.2 SigningTime

A.2.1 General

This element shall be used to report on the claimed signing time in the signature.

A.2.2 XML

The signing time shall be reported on in the `SigningTime` element.

The `SigningTime` element shall be of type `SASigningTimeType`.

```
<xs:complexType name="SASigningTimeType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="Time" type="xs:dateTime"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

A.2.3 CAdES

The `Time` element within the `SASigningTimeType` shall contain the time as contained in the `signing-time` attribute.

A.2.4 XAdES

The `Time` element within the `SASigningTimeType` shall contain the time as contained in the `XAdES:SigningTime` qualifying property.

A.2.5 PAdES

For PAdES signatures as specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5, the `Time` element within the `SASigningTimeType` shall contain the time value present in the `M` entry of the Signature PDF dictionary.

For PAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.3 SigningCertificate

A.3.1 General

This element shall be used to report on the references to the signing certificate path.

A.3.2 XML

The reference to the signing certificate path shall be reported on in the `SigningCertificate` element.

The `SigningCertificate` element shall be of type `SACertIDListType`.

```
<xs:complexType name="SACertIDListType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="CertID" type="vr:SACertIDType" minOccurs="0"
                            maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

<xs:complexType name="SACertIDType">
    <xs:sequence>
        <xs:element name="X509IssuerSerial" type="xs:base64Binary" minOccurs="0"/>
        <xs:element ref="ds:DigestMethod" />
        <xs:element ref="ds:DigestValue" />
    </xs:sequence>
</xs:complexType>
```

For every certificate referenced within reported attribute that is present in a validation object in the report, the `SigningCertificate` shall contain an `AttributeObject` child referencing the validation object containing the corresponding certificate.

For every certificate referenced within the reported attribute that is not present as validation object (for instance because the creator of the validation report cannot gain access to it), this component shall have one `CertID` child.

The `ds:DigestValue` and `ds:DigestMethod` children shall contain the digest value and algorithm indicated in the corresponding certificate reference.

The `X509IssuerSerial` element shall be the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035 [12].

A.3.3 CAdES

For every element in `certs` of type `ESSCertID` in the `signing-certificate` attribute or of type `ESSCertIDv2` element in the `signing-certificate-v2` attribute, for which the referenced certificate is not presented by an `AttributeObject` child referencing the validation object containing the corresponding certificate, the `SigningCertificate` in the report shall contain one `CertID` child.

If the element of type `ESSCertID` is reported by a `CertID` child then:

1) The `ds:DigestValue` value shall be the base-64 encoding octet string contained in the `certHash` field in the instance of the `ESSCertID` type.

2) The `ds:DigestMethod` shall have the value `http://www.w3.org/2000/09/xmldsig#sha1`.

3) If the `issuerSerial` element is present within the element of type `ESSCertID`, then the `X509IssuerSerial` element shall be the base-64 encoding of one DER-encoded `issuerSerial` field in instance of `ESSCertID` type.

If the element of type `ESSCertIDV2` is reported by a `CertID` child then:

1) The `ds:DigestValue` value shall be the base-64 encoding of the octet string contained in the `certHash` field in the instance of the `ESSCertID` type.

2) The `ds:DigestMethod` shall have as value an URN. This URN shall represent the OID value present in the `hashAlgorithm` field in the instance of the `ESSCertIDV2` type. The URN shall be built as specified in IETF RFC 3061 [8].

3) If the `issuerSerial` element is present within the element of type `ESSCertIDV2`, then the `X509IssuerSerial` element shall be the base-64 encoding of one DER-encoded `issuerSerial` field in instance of `ESSCertID` type.

A.3.4 XAdES

For every certificate referenced within the `XAdES:SigningCertificateV2` in the reported XAdES signature, for which the referenced certificate is not presented by an `AttributeObject` child referencing the validation object containing the corresponding certificate, the `SigningCertificate` in the report shall contain one `CertID` child.

If the certificate referenced within the `XAdES:SigningCertificateV2` is reported by a `CertID` child then:

1) The `ds:DigestValue` and `ds:DigestMethod` shall contain the values indicated in the reference certificate as in the `XAdES:SigningCertificateV2` qualifying property of the signature.

2) `X509IssuerSerial` element shall be the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035 [12], as present within `IssuerSerialV2` within `XAdES:SigningCertificateV2` qualifying property.

A.3.5 PAdES

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5, the same rules as for CAdES signatures shall apply.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 may contain the `XAdES:SigningCertificateV2` qualifying property. In these cases, this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.4 DataObjectFormat

A.4.1 General

This element shall be used to report on the format of the signed data.

A.4.2 XML

The data object format shall be reported on in the `DataObjectFormat` element.

The `DataObjectFormat` element shall be of type `SADataObjectFormatType`.

```
<xs:complexType name="SADataObjectFormatType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="ContentType" type="xs:anyURI" minOccurs="0"/>
                <xs:element name="MimeType" type="xs:string" minOccurs="0"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

A.4.3 CAdES

The `ContentType` element shall contain the OID contained in the `content-type` attribute, represented as URN as described in IETF RFC 3061 [8].

The `MimeType` element shall contain the UTF8String as contained in the `mime-type` attribute.

A.4.4 XAdES

The `ContentType` child element shall contain the URI present within the `XAdES:Identifier` child element of `XAdES:ObjectIdentifier` child element of `XAdES:DataObjectFormat` qualifying property of XAdES.

The `MimeType` shall contain the value of `XAdES:MimeType` child element of the `XAdES:DataObjectFormat` qualifying property of XAdES.

A.4.5 PAdES

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5, the same rules as for CAdES signatures shall apply.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 may contain the `XAdES:DataObjectFormat` qualifying property. In these cases, this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.5 CommitmentTypeIndication

A.5.1 General

This element shall be used to report on the commitment type contained in the signature.

A.5.2 XML

The commitment type shall be reported on in the `CommitmentTypeIndication` element.

The `CommitmentTypeIndication` element shall be of type `SACommitmentTypeIndicationType`.

```
<xs:complexType name="SACommitmentTypeIndicationType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="CommitmentTypeIdentifier" type="xs:anyURI"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

A.5.3 CAdES

The `CommitmentTypeIdentifier` element shall contain the OID of the `CommitmentTypeId` in the `commitment-type-indication` attribute, represented as URN as described in IETF RFC 3061 [8].

A.5.4 XAdES

The `CommitmentTypeIdentifier` child element shall contain the URI present within the `XAdES:Identifier` child element of `XAdES:CommitmentTypeId` child element of `XAdES:CommitmentTypeIndication` qualifying property of XAdES.

A.5.5 PAdES

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 the same rule as for CAdES signatures shall apply.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

NOTE: The information within the key `Reason` is specified in clause A.30.

A.6 AllDataObjectsTimeStamp

A.6.1 General

This element shall be used to on a time-stamp on all data objects covered by the signature.

A.6.2 XML

The signed attributed containing the time stamp on all data objects which are signed shall be reported on in the `AllDataObjectsTimeStamp` element.

The `AllDataObjectsTimeStamp` element shall be of type `SATimestampType`.

NOTE: `SATimestampType` is used for other time-stamps as well and defined here.

```
<xs:complexType name="SATimestampType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
```

```
                    <xs:element name="TimeStampValue" type="xs:dateTime"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
```

A.6.3 CAdES

The `TimeStampValue` shall contain the time indicated in the time-stamp token contained in the `content-time-stamp` attribute.

The `AttributeObject` shall contain a reference to the validation object containing the time-stamp contained in the `content-time-stamp` attribute.

A.6.4 XAdES

The `TimeStampValue` child element shall contain the time indicated in the time-stamp token contained in the `XAdES:AllDataObjectsTimeStamp` qualifying property of XAdES.

The `AttributeObject` shall contain a reference to the validation object containing the time-stamp contained in the `XAdES:AllDataObjectsTimeStamp` qualifying property.

A.6.5 PAdES

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 the same rule as for CAdES signatures shall apply.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.7 IndividualDataObjectsTimeStamp

A.7.1 General

This element shall be used to report on time-stamps on individual data objects in signatures that may cover several data objects. For each time-stamp token one `IndividualDataObjectsTimeStamp` element shall be added.

EXAMPLE: XAdES signatures can sign multiple data objects.

A.7.2 XML

The time stamp on individual data objects shall be reported on in the `IndividualDataObjectsTimeStamp` element.

The `IndividualDataObjectsTimeStamp` element shall be of type `SATimestampType`.

A.7.3 XAdES

The `TimeStampValue` child element shall contain the time indicated in the time-stamp token contained in the `XAdES:IndividualDataObjectsTimeStamp` qualifying property of XAdES.

The `AttributeObject` shall contain a reference to the validation object containing the time-stamp contained in the `XAdES:IndividualDataObjectsTimeStamp` qualifying property.

A.7.4 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 are based on CAdES signatures. Consequently, this component is not present when reporting on PAdES signatures.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.8 SignaturePolicyIdentifier

A.8.1 General

This element shall be used to report on the signature policy identifier contained in the signature.

A.8.2 XML

The signature policy identifier shall be reported on in the `SignaturePolicyIdentifier` element.

The `SignaturePolicyIdentifier` element shall be of type `SASignaturePolicyIdentifierType`.

```
    <xs:complexType name="SASignaturePolicyIdentifierType">
        <xs:complexContent>
            <xs:extension base="vr:AttributeBaseType">
                <xs:sequence>
                    <xs:element name="SignaturePolicyID" type="xs:anyURI"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
```

A.8.3 CAdES

The element `SignaturePolicyID` shall contain the OID contained in `sigPolicyId` in the `signature-policy-identifier` attribute, represented as URN as described in IETF RFC 3061 [8].

A.8.4 XAdES

The `SignaturePolicyID` child element shall contain the URI present within the `XAdES:Identifier` child element of `XAdES:SigPolicyId` child element of `XAdES:SignaturePolicyId` child element of `XAdES:CommitmentTypeIndication` qualifying property of XAdES.

A.8.5 PAdES

For PAdES signatures as specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 the same rule as for CAdES signatures shall apply.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.9 SignatureProductionPlace

A.9.1 General

This element shall be used to report on the place where the signature is claimed to have been created.

A.9.2 XML

The claimed signature production place shall be reported on in the `SignatureProductionPlace` element.

The `SignatureProductionPlace` element shall be of type `SASignatureProductionPlaceType`.

```
<xs:complexType name="SASignatureProductionPlaceType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="AddressString" type="xs:string" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

A.9.3 CAdES

If `countryName` is contained in the `signer-location` attribute, the contained `DirectoryString` shall be reported in one `AddressString` entry.

If `localityName` is contained in the `signer-location` attribute, the contained `DirectoryString` shall be reported in one `AddressString` entry.

If `postalAddress` is contained in the `signer-location` attribute, every contained `DirectoryString` shall be reported in one separate `AddressString` entry.

A.9.4 XAdES

Each of the child-elements of the XAdES attributes reporting the location where the signature has been purportedly generated shall be reported in one `AddressString` entry.

EXAMPLES: `XAdES:City, XAdES:StreetAddress, XAdES:StateOrProvince, XAdES:PostalCode, XAdES:CountryName`

A.9.5 PAdES

For PAdES signatures as specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 this component shall have the contents of the `Location` entry in the Signature PDF dictionary.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.10 SignerRole

A.10.1 General

This element shall be used to report on a certified or claimed role of the signer.

A.10.2 XML

The certified or claimed role of the signer shall be reported on in the `SignerRole` element.

The `SignerRole` element shall be of type `SASignerRoleType`.

```
<xs:complexType name="SASignerRoleType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
```

```
            <xs:sequence>
                <xs:element name="RoleDetails" type="vr:SAOneSignerRoleType"
                            maxOccurs="unbounded" />
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

<xs:complexType name="SAOneSignerRoleType">
    <xs:sequence>
        <xs:element name="Role" type="xs:string"/>
        <xs:element name="EndorsementType">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="certified"/>
                    <xs:enumeration value="claimed"/>
                    <xs:enumeration value="signed"/>

                </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>
```

A.10.3 CAdES

For every instance of `Attribute` in `claimedAttributes` of the `signer-attributes-v2` attribute, the `SignerRole` element shall contain one `RoleDetails` child element. It shall have the `EndorsementType` set to `claimed` and `Role` containing a string representation of the `Attribute` instance. The string representation of the `Attribute` instance is left to the creator of the report.

For every instance of `AttributeCertificate` or `OtherAttributeCertificate` in `certifiedAttributesV2` of the `signer-attributes-v2` attribute, the `SignerRole` element shall contain one `RoleDetails` child element. It shall have the `EndorsementType` set to `certified` and `Role` containing a string representation of the `AttributeCertificate` or `OtherAttributeCertificate` instance. The string representation of the `AttributeCertificate` or `OtherAttributeCertificate` instance is left to the creator of the report.

For every instance of `SignedAssertion` in signedAssertions of the `signer-attributes-v2` attribute, the `SignerRole` element shall contain one `RoleDetails` child element. It shall have the `EndorsementType` set to `signed` and `Role` containing a string representation of the `SignedAssertion` instance. The string representation of the `SignedAssertion` instance is left to the creator of the report.

A.10.4 XAdES

For every `ClaimedRole` child element of `ClaimedRoles` child element of `XAdES:SignerRole` or `XAdES:SignerRoleV2` qualifying properties, this component shall have one `RoleDetails` child element. It shall have the `EndorsementType` set to `claimed` and `Role` containing a string representation of the `Attribute` instance. The string representation of the `Attribute` instance is left to the creator of the report.

For every `CertifiedRole` child element of `CertifiedRoles` child element of `XAdES:SignerRole` and for every `CertifiedRole` child element of `CertifiedRolesV2` child element of `XAdES:SignerRoleV2` qualifying properties, this component shall have one `RoleDetails` child element. It shall have the `EndorsementType` set to `certfied` and `Role` containing a string representation of the `Attribute` instance. The string representation of the `AttributeCertificate` or `OtherAttributeCertificate` instance is left to the creator of the report.

For every `SignedAssertion` child element of `SignedAssertions` child element of `XAdES:SignerRoleV2` qualifying properties, this component shall have one `RoleDetails` child element. It shall have the `EndorsementType` set to `signed` and `Role` containing a string representation of the `Attribute` instance. The string representation of the `SignedAssertion` instance is left to the creator of the report.

A.10.5 PAdES

For PAdES signatures as specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 the same rule as for CAdES signatures shall apply.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.11 CounterSignature

A.11.1 General

This element shall be used to report on a counter signature.

A.11.2 XML

The certified or claimed role of the signer shall be reported on in the `CounterSignature` element.

The `CounterSignature` element shall be of type `SACounterSignatureType`.

```
    <xs:complexType name="SACounterSignatureType">
        <xs:complexContent>
            <xs:extension base="vr:AttributeBaseType">
                <xs:sequence>
                    <xs:element name="CounterSignature" type="vr:SignatureReferenceType"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
```

A.11.3 CAdES

The `AttributeObject` shall contain a reference to the validation object containing the signature contained in the `counter-signature` attribute.

A.11.4 XAdES

The `AttributeObject` shall contain a reference to the validation object containing the signature contained in the `XAdES:CounterSignature` qualifying attribute or to a detached countersignature of the XAdES signature.

A.11.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the `counter-signature` attribute. Consequently, this component is not present when reporting on PAdES signatures.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.12 SignatureTimeStamp

A.12.1 General

This element shall be used to report on a signature time-stamp.

A.12.2 XML

The signature time-stamp shall be reported on in the `SignatureTimeStamp` element.

The `SignatureTimeStamp` element shall be of type `SATimestampType`.

A.12.3 CAdES

The `TimeStampValue` shall contain the time of the time-stamp contained in the `signature-time-stamp` attribute.

The `AttributeObject` shall contain a reference to the validation object containing the time-stamp contained in the `signature-time-stamp` attribute.

A.12.4 XAdES

The `TimeStampValue` shall contain the time of the time-stamp contained in the `XAdES:SignatureTimeStamp` qualifying property.

The `AttributeObject` shall contain a reference to the validation object containing the time-stamp contained in the `XAdES:SignatureTimeStamp` qualifying property.

A.12.5 PAdES

For PAdES signatures as specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 the same rule as for CAdES signatures shall apply.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.13 CompleteCertificateRefs

A.13.1 General

This element shall be used to report on the references to certificates used in the signature.

A.13.2 XML

The certificate references shall be reported on in the `CompleteCertificateRefs` element.

The `CompleteCertificateRefs` element shall be of type `SACertIDListType`.

The same requirements as in clause A.3.2 shall apply.

A.13.3 CAdES

For every element type `OtherCertID` in the `complete-certificate-references` attribute, for which the referenced certificate is not presented by an `AttributeObject` child referencing the validation object containing the corresponding certificate, the `CompleteCertificateRefs` in the report shall contain one `CertID` child.

If the element of type `OtherCertID` is reported by a `CertID` child then:

1) If the `otherCertHash` contains the element `sha1Hash`, then:

   a) The `ds:DigestValue` value shall be the base-64 encoding of the octet string contained in the `sha1Hash` field.

   b) The `ds:DigestMethod` shall have the value `http://www.w3.org/2000/09/xmldsig#sha1.`

2) If the `otherCertHash` contains the element `otherHash`, then:

   a) The `ds:DigestValue` value shall be the base-64 encoding of the octet string contained in the `hashValue` field within the `otherHash` field.

   b) The `ds:DigestMethod` shall have as value an URN. This URN shall represent the OID value present in the `hashAlgorithm` field within the `otherHash` field. The URN shall be built as specified in IETF RFC 3061 [8].

3) If the `issuerSerial` element is present within the element of type `OtherCertID`, then the `X509IssuerSerial` element shall be the base-64 encoding of one DER-encoded `issuerSerial` field.

A.13.4 XAdES

For every certificate referenced within the `XAdES:CompleteCertificateRefsV2` qualifying property in the reported XAdES signature, for which the referenced certificate is not presented by an `AttributeObject` child referencing the validation object containing the corresponding certificate, the `CompleteCertificateRefs` in the report shall contain one `CertID` child.

If the certificate referenced within the `XAdES:CompleteCertificateRefsV2` is reported by a `CertID` child then:

1) The `ds:DigestValue` and `ds:DigestMethod` shall contain the values indicated in the referenced certificate as in the `XAdES:CompleteCertificateRefsV2` qualifying property of the signature.

2) The `X509IssuerSerial` element shall be the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035 [12], as present within `IssuerSerialV2` within `XAdES:CompleteCertificateRefsV2` qualifying property.

A.13.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the `complete-certificate-references` attribute. Consequently, this component is not present when reporting on PAdES signatures.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.14 CompleteRevocationRefs

A.14.1 General

This element allows reporting on the reference on revocation information which can be used to validate the signature.

A.14.2 XML

The references to the revocation information shall be reported on in the `CompleteRevocationRefs` element.

The `CompleteRevocationRefs` element shall be of type `SARevIDListType`.

```
<xs:complexType name="SARevIDListType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:choice minOccurs="0" maxOccurs="unbounded">
                <xs:element name="CRLID" type="vr:SACRLIDType" />
                <xs:element name="OCSPID" type="vr:SAOCSPIDType" />
            </xs:choice>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="SACRLIDType">
    <xs:sequence>
        <xs:element ref="ds:DigestMethod" />
        <xs:element ref="ds:DigestValue" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="SAOCSPIDType">
    <xs:sequence>
        <xs:element name="ProducedAt" type="xs:dateTime" />
        <xs:choice>
            <xs:element name="ResponderIDByName" type="xs:string"  />
            <xs:element name="ResponderIDByKey" type="xs:base64Binary"  />
        </xs:choice>
    </xs:sequence>
</xs:complexType>
```

For every CRL or OCSP response referenced within reported attribute that is present in a validation object in the report, the `CompleteRevocationRefs` shall contain an `AttributeObject` child referencing the validation object containing the corresponding certificate.

For every CRL referenced within the reported attribute that is not present as validation object (for instance because the creator of the validation report cannot gain access to it), this component shall have one `CRLID` child. Its `ds:DigestMethod` shall contain an URI identifying the same digest algorithm as the one present in the attribute of the reported signature. Its `ds:DigestValue` shall contain the base-64 encoding of the digest value present in the attribute of the reported signature.

For every OCSP response referenced within the reported attribute that is not present as validation object (for instance because the creator of the validation report cannot gain access to it), this component shall have one `OCSPID` child.

A.14.3 CAdES

For every element in `crlids` of `complete-revocation-references`, referencing a CRL that is not present in the validation report, the `CompleteRevocationRefs` in the report shall contain one `CRLID` child.

For every element in `ocspids` of `complete-revocation-references`, referencing an OCSP response that is not present in the validation report, the `CompleteRevocationRefs` in the report shall contain one `OCSPID` child. Its `ProducedAt` child shall contain the same time value as the value indicated in the `producedAt` in the aforementioned element in `ocspids`. The `ResponderIDByKey` shall have the base-64 encoding of the value present in the `ocspResponderID` when its choice is `ByKey` in in the aforementioned element in `ocspids`. The `ResponderIDByName` shall have the string representation of the value present in the `ocspResponderID` when its choice is `ByKey` in the aforementioned element in `ocspids`.

A.14.4 XAdES

For every element in `CRLRefs` of `CompleteRevocationRefs`, referencing a CRL that is not present in the validation report, the `CompleteRevocationRefs` in the report shall contain one `CRLID` child.

For every element in OCSPRefs of CompleteRevocationRefs, referencing an OCSP response that is not present in the validation report, the CompleteRevocationRefs in the report shall contain one OCSPID child. Its ProducedAt child shall contain the same time value as the value indicated in the XAdES:ProducedAt in the aforementioned element in OCSPRefs. The ResponderIDByKey shall have the base-64 encoding of the value present in the XAdES:ByKey in the aforementioned element in OCSPRefs. The ResponderIDByName shall have the same value as the value of OCSPRefs. The ResponderIDByKey shall have the base-64 encoding of the value present in the XAdES:ByName in the aforementioned element in OCSPRefs.

A.14.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the complete-revocation-references attribute. Consequently, this component is not present when reporting on PAdES signatures.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.15 AttributeCertificateRefs

A.15.1 General

This element shall be used to report on the references to attribute certificates used in the signature.

A.15.2 XML

The certificate references shall be reported on in the AttributeCertificateRefs element.

The AttributeCertificateRefs element shall be of type SACertIDListType.

The same requirements as in clause A.3.2 shall apply.

A.15.3 CAdES

For every element type OtherCertID in attribute-certificate-references attribute, for which the referenced certificate is not presented by an AttributeObject child referencing the validation object containing the corresponding certificate, the CompleteCertificateRefs in the report shall contain one CertID child.

If the element of type OtherCertID is reported by a CertID child then:

1) If the otherCertHash contains the element sha1Hash, then:

   a) The ds:DigestValue value shall be the base-64 encoding of the octet string contained in the sha1Hash field.

   b) The ds:DigestMethod shall have the value http://www.w3.org/2000/09/xmldsig#sha1.

2) If the otherCertHash contains the element otherHash, then:

   a) The ds:DigestValue value shall be the base-64 encoding of the octet string contained in the hashValue field within the otherHash field.

   b) The ds:DigestMethod shall have as value an URN. This URN shall represent the OID value present in the hashAlgorithm field within the otherHash field. The URN shall be built as specified in IETF RFC 3061 [8].

3) If the `issuerSerial` element is present within the element of type `OtherCertID`, then the `X509IssuerSerial` element shall be the base-64 encoding of one DER-encoded `issuerSerial` field.

A.15.4 XAdES

For every certificate referenced within the `XAdES:AttributeCertificateRefsV2` qualifying property in the reported XAdES signature, for which the referenced certificate is not presented by an `AttributeObject` child referencing the validation object containing the corresponding certificate, the `CompleteCertificateRefs` in the report shall contain one `CertID` child.

If the certificate referenced within the `XAdES: AttributeCertificateRefsV2` is reported by a `CertID` child then:

1) The `ds:DigestValue` and `ds:DigestMethod` shall contain the values indicated in the referenced certificate as in the `XAdES: AttributeCertificateRefsV2` qualifying property of the signature.

2) The `X509IssuerSerial` element shall be the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035 [12], as present within `IssuerSerialV2` within `XAdES:AttributeCertificateRefsV2` qualifying property.

A.15.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the `attribute-certificate-references` attribute. Consequently, this component is not present when reporting on PAdES signatures.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.16 AttributeRevocationRefs

A.16.1 General

This element allows reporting on the contents of the `XAdES:AttributeRevocationRefs` qualifying property of XAdES signatures and the `attribute-revocation-references` attribute of CAdES signatures.

A.16.2 XML

The certificate references shall be reported on in the `AttributeRevocationRefs` element.

The `AttributeRevocationRefs` element shall be of type `SARevIDListType`.

The same requirements as in clause A.14.2 shall apply.

A.16.3 CAdES

For every element in `crlids` of `attribute-revocation-references`, referencing a CRL that is not present in the validation report, the `CompleteRevocationRefs` in the report shall contain one `CRLID` child.

For every element in `ocspids` of `attribute-revocation-references`, referencing an OCSP response that is not present in the validation report, the `CompleteRevocationRefs` in the report shall contain one `OCSPID` child. Its `ProducedAt` child shall contain the same time value as the value indicated in the `producedAt` in the aforementioned element in `ocspids`. The `ResponderIDByKey` shall have the base-64 encoding of the value present in the `ocspResponderID` when its choice is `ByKey` in in the aforementioned element in `ocspids`.

The ResponderIDByName shall have the string representation of the value present in the ocspResponderID when its choice is ByKey in the aforementioned element in ocspids.

A.16.4 XAdES

For every element in CRLRefs of AttributeRevocationRefs, referencing a CRL that is not present in the validation report, the CompleteRevocationRefs in the report shall contain one CRLID child.

For every element in OCSPRefs of AttributeRevocationRefs, referencing an OCSP response that is not present in the validation report, the CompleteRevocationRefs in the report shall contain one OCSPID child. Its ProducedAt child shall contain the same time value as the value indicated in the XAdES:ProducedAt in the aforementioned element in OCSPRefs. The ResponderIDByKey shall have the base-64 encoding of the value present in the XAdES:ByKey in the aforementioned element in OCSPRefs. The ResponderIDByName shall have the same value as the value of OCSPRefs. The ResponderIDByKey shall have the base-64 encoding of the value present in the XAdES:ByName in the aforementioned element in OCSPRefs.

A.16.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the attribute-revocation-references attribute. Consequently, this component is not present when reporting on PAdES signatures.

For XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6 the same rule as for XAdES signatures shall apply.

A.17 SigAndRefsTimeStamp

A.17.1 General

This element shall be used to report on a time-stamp covering the signature and the references on certificates and revocation information.

A.17.2 XML

The time-stamp on the signature and the references on certificates and revocation information shall be reported on in the SigAndRefsTimeStamp element.

The SigAndRefsTimeStamp element shall be of type SATimestampType.

A.17.3 CAdES

The TimeStampValue shall contain the time of the time-stamp contained in the CAdES-C-time-stamp attribute.

The AttributeObject shall contain a reference to the validation object containing the time-stamp contained in the CAdES-C-time-stamp attribute.

A.17.4 XAdES

The TimeStampValue shall contain the time of the time-stamp contained in the XAdES:SigAndRefsTimeStampV2 qualifying property.

The AttributeObject shall contain a reference to the validation object containing the time-stamp contained in the XAdES:SigAndRefsTimeStampV2 qualifying property.

A.17.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the `CAdES-C-time-stamp` attribute. Consequently, this component is not present when reporting on PAdES signatures.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6.2 may contain the `XAdES:SigAndRefsTimeStampV2`. In these cases, this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.18 RefsOnlyTimeStamp

A.18.1 General

This element can be used to report on the time-stamp covering the references on certificates and revocation information.

A.18.2 XML

The time-stamp on the references on certificates and revocation information shall be reported on in the `SigAndRefsTimeStamp` element.

The `SigAndRefsTimeStamp` element shall be of type `SATimestampType`.

A.18.3 CAdES

The `TimeStampValue` shall contain the time of the time-stamp contained in the `time-stamped-certs-crls-references` attribute.

The `AttributeObject` shall contain a reference to the validation object containing the time-stamp contained in the `time-stamped-certs-crls-references` attribute.

A.18.4 XAdES

The `TimeStampValue` shall contain the time of the time-stamp contained in the `XAdES:RefsOnlyTimeStampV2` qualifying property.

The `AttributeObject` shall contain a reference to the validation object containing the time-stamp contained in the `XAdES:RefsOnlyTimeStampV2` qualifying property.

A.18.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the `time-stamped-certs-crls-references` attribute. Consequently, this component is not present when reporting on PAdES signatures.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6.2 may contain `XAdES:RefsOnlyTimeStampV2` qualifying property. In these cases, this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.19 CertificateValues

A.19.1 General

This element shall be used to report on the attribute containing the certificates used in the signature.

A.19.2 XML

The certificates within such an attribute shall be reported on in the `CertificateValues` element.

The `CertificateValues` element shall be of type `AttributeBaseType`.

A.19.3 CAdES

For every instance of `Certificate` contained in the `certificate-values` attribute, the `CertificateValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding certificate.

A.19.4 XAdES

For every instance child element present in the `XAdES:CertificateValues` qualifying property, the `CertificateValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding certificate.

A.19.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the `certificate-values` attribute. Consequently, this component is not present when reporting on PAdES signatures.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6.2 may contain `XAdES:CertificateValues` qualifying property. In these cases this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.20 RevocationValues

A.20.1 General

This element shall be used to report on the attribute containing the revocation information corresponding to the signature.

A.20.2 XML

The revocation information within such an attribute shall be reported on in the `RevocationValues` element.

The `RevocationValues` element shall be of type `AttributeBaseType`.

A.20.3 CAdES

For every instance of `CertificateList` contained in the `revocation-values` attribute, the `RevocationValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding CRL.

For every instance of `BasicOCSPResponse` contained in the `revocation-values` attribute, the `RevocationValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding OCSP response.

For every item of `otherRevVals` contained in the `revocation-values` attribute, the `RevocationValues` element shall contain an `AttributeObject` referencing the corresponding validation object.

A.20.4 XAdES

For every child element of the `XAdES:CRLValues` child element of `XAdES:RevocationValues` qualifying property, the `RevocationValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding CRL.

For every child element of the `XAdES:OCSPValues` child element of `XAdES:RevocationValues` qualifying property, the `RevocationValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding OCSP response.

For every child element of the `XAdES:OtherValues` child element of `XAdES:RevocationValues` qualifying property, the `RevocationValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding validation data object.

A.20.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not have the `revocation-values` attribute. Consequently, this component is not be present when reporting on PAdES signatures.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6.2 may contain `XAdES:RevocationValues` qualifying property. In these cases, this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.21 AttrAuthoritiesCertValues

A.21.1 General

This element shall be used to report on an attribute containing certificates to be used in the validation of attribute certificates or signed assertions.

A.21.2 XML

The certificates within such an attribute shall be reported on in the `AttrAuthoritiesCertValues` element.

The `AttrAuthoritiesCertValues` element shall be of type `AttributeBaseType`.

A.21.3 XAdES

For every instance child element present in the `XAdES:AttrAuthoritiesCertValues` qualifying property, the `CertificateValues` element shall contain an `AttributeObject` referencing the validation object containing corresponding certificate.

A.21.4 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 are based on CAdES signatures. Consequently, this component is not present when reporting on PAdES signatures.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6.2 may contain the `XAdES:AttrAuthoritiesCertValues` qualifying property. In these cases, this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.22 AttributeRevocationValues

A.22.1 General

This element shall be used to report on attributes containing revocation information to be used in the validation of attribute certificates or signed assertions.

A.22.2 XML

The revocation information within such an attribute shall be reported on in the `AttributeRevocationValues` element.

The `AttributeRevocationValues` element shall be of type `AttributeBaseType`.

A.22.3 XAdES

For every child element of the `XAdES:CRLValues` child element of `XAdES:AttributeRevocationValues` qualifying property, the `RevocationValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding CRL.

For every child element of the `XAdES:OCSPValues` child element of `XAdES:AttributeRevocationValues` qualifying property, the `RevocationValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding OCSP response.

For every child element of the `XAdES:OtherValues` child element of `XAdES:AttributeRevocationValues` qualifying property, the `RevocationValues` element shall contain an `AttributeObject` referencing the validation object containing the corresponding validation data object.

A.22.4 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 are based on CAdES signatures. Consequently, this component is not present when reporting on PAdES signatures.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6.2 may contain `XAdES:AttributeRevocationValues` qualifying property. In these cases this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.23 TimeStampValidationData

A.23.1 General

This element shall be used to report on attributes containing certificates and revocation information to be used to validate a time-stamp.

A.23.2 XML

The certificates and revocation information within such an attribute shall be reported on in the `TimeStampValidationData` element.

The TimeStampValidationData element shall be of type AttributeBaseType.

A.23.3 XAdES

The certificates present in the XAdES:CertificateValues child element of XAdES:TimeStampValidationData qualifying property shall be reported in the TimeStampValidation component as the certificates present in XAdES:CertificateValues qualifying property.

The revocation values present in the XAdES:RevocationValues child element of XAdES:TimeStampValidationData qualifying property shall be reported in the TimeStampValidation component as the revocation values present in XAdES:RevocationValues qualifying property.

A.23.4 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 are based on CAdES signatures. Consequently, this component is not present when reporting on PAdES signatures.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6.2 may contain XAdES:AttributeRevocationValues qualifying property. In these cases, this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.24 ArchiveTimeStamp

A.24.1 General

This element shall be used to report on an archival time-stamp.

A.24.2 XML

The time-stamp on the references on certificates and revocation information shall be reported on in the ArchiveTimeStamp element.

The ArchiveTimeStamp element shall be of type SATimestampType.

A.24.3 CAdES

For every archive-time-stamp-v3 attribute, an ArchiveTimeStamp element shall be added to the report.

The TimeStampValue shall contain the time of the time-stamp contained in the archive-time-stamp-v3 attribute.

The AttributeObject shall contain a reference to the validation object containing the time-stamp contained in the archive-time-stamp-v3 attribute.

For every archive-time-stamp attribute, an ArchiveTimeStamp element shall be added to the report.

The TimeStampValue shall contain the time of the time-stamp contained in the archive-time-stamp attribute.

The AttributeObject shall contain a reference to the validation object containing the time-stamp contained in the archive-time-stamp attribute.

For every long-term-validation attribute, an ArchiveTimeStamp element shall be added to the report.

The TimeStampValue shall contain the time of the time-stamp or evidence record contained in the long-term-validation attribute.

The AttributeObject shall contain a reference to the validation object containing the time-stamp or evidence record contained in the long-term-validation attribute.

A.24.4 XAdES

For every time-stamp token present in a XAdES:ArchiveTimeStamp qualifying property defined in the namespace whose URI is http://uri.etsi.org/01903/v1.4.1# and for every time-stamp token present in a XAdES:ArchiveTimeStamp qualifying property defined in the namespace whose URI is http://uri.etsi.org/01903/v1.3.2# there shall be one ArchiveTimeStamp component whose AttributeObject shall contain a reference to the validation object containing the time-stamp token.

A.24.5 PAdES

PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 do not contain the archive-time-stamp-v3 attributes or archive-time-stamp attributes. Consequently, this component is not present when reporting on PAdES signatures.

XAdES signatures as specified in ETSI EN 319 142-2 [i.4], clause 6.2 may contain XAdES:ArchiveTimeStamp qualifying property. In these cases this component may be present and the requirements are as the ones specified for reporting on any other XAdES signature.

A.25 RenewedDigests

A.25.1 General

This element shall be used to report on the XAdES:RenewedDigests qualifying property of XAdES signatures.

A.25.2 XML

The time-stamp on the references on certificates and revocation information shall be reported on in the RenewedDigests element.

The RenewedDigests element shall be of type SAListOfIntegers.

```
    <xs:complexType name="SAListOfIntegers">
        <xs:complexContent>
            <xs:extension base="vr:AttributeBaseType">
                <xs:element name="ListOfIntegers" type="vr:ListOfIntegersType" />
        </xs:complexContent>
    </xs:complexType>
    <xs:simpleType name="ListOfIntegersType">
        <xs:list itemType="xs:integer"/>
    </xs:simpleType>
```

A.25.3 XAdES

When the reported signature is a XAdES signature, each integer value present in this component shall identify the order of appearance of the ds:Reference whose digest has been renewed when the XAdES signature is serialized, where the value "1" is assigned to the first ds:Reference child of the ds:SignedInfo element.

A.26 MessageDigest

A.26.1 General

This element shall be used to report on the attribute containing the message digest of the content being signed.

A.26.2 XML

The message digest shall be reported on in the `MessageDigest` element.

The `MessageDigest` element shall be of type `SAMessageDigestType`.

```
<xs:complexType name="SAMessageDigestType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="Digest" type="xs:base64Binary"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

A.26.3 CAdES

The `Digest` element shall contain the octet string contained in `message-digest` attribute.

A.26.4 PAdES

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 the same rule as for CAdES signatures shall apply.

A.27 DSS

A.27.1 General

This element shall be used to report the contents of the DSS PDF dictionary.

A.27.2 XML

The contents of the DSS PDF dictionary shall be reported on in the `DSS` element.

The `DSS` element shall be of type `SADSSType`.

```
<xs:complexType name="SADSSType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="Certs" type="vr:VOReferenceType" minOccurs="0"/>
                <xs:element name="CRLs" type="vr:VOReferenceType" minOccurs="0"/>
                <xs:element name="OCSPs" type="vr:VOReferenceType" minOccurs="0"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

`Certs` child shall contain a sequence of references to validation objects, each one containing one certificate.

`CRLs` child shall contain a sequence of references to validation objects, each one containing one CRL.

`OCSPs` child shall contain a sequence of references to validation objects, each one containing one OCSP response.

A.27.3 PAdES

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 each `AttributeObject` child element of `Certs` child element in `DSS` component shall contain a reference to one validation object containing one certificate present in the DSS PDF dictionary of the PAdES signature. Every certificate present in this PDF dictionary shall be referenced by one of the aforementioned `AttributeObject` elements.

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 each `AttributeObject` child element of `CRLs` child element in `DSS` component shall contain a reference to one validation object containing one CRL present in the DSS PDF dictionary of the PAdES signature. Every CRL present in this PDF dictionary shall be referenced by one of the aforementioned `AttributeObject` elements.

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 each `AttributeObject` child element of `OCSPs` child element in `DSS` component shall contain a reference to one validation object containing one OCSP response present in the DSS PDF dictionary of the PAdES signature. Every OCSP response present in this PDF dictionary shall be referenced by one of the aforementioned `AttributeObject` elements.

A.28 VRI

A.28.1 General

This element shall be used to report on the certificate references contained in the VRI Dictionary.

A.28.2 XML

The contents of the VRI PDF dictionary shall be reported on in the `VRI` element.

The `VRI` element shall be of type `SAVRIType`.

```
<xs:complexType name="SAVRIType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="Certs" type="vr:VOReferenceType" minOccurs="0"/>
                <xs:element name="CRLs" type="vr:VOReferenceType" minOccurs="0"/>
                <xs:element name="OCSPs" type="vr:VOReferenceType" minOccurs="0"/>
                <xs:element name="TU" type="xs:string" minOccurs="0"/>
                <xs:element name="TS" type="vr:SATimeStampType" minOccurs="0"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

The `Certs` child shall contain a sequence of references to validation objects, each one containing one certificate.

The `CRLs` child shall contain a sequence of references to validation objects, each one containing one CRL.

The `OCSPs` child shall contain a sequence of references to validation objects, each one containing one OCSP response.

The `TU` child shall contain a date string as defined in ISO 32000-1 [9].

The `TS` child shall contain reference to a validation object containing a time-stamp token.

A.28.3 PAdES

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 each `AttributeObject` child element of the `Certs` child element in a `VRI` component shall contain a reference to one validation object containing one certificate present in one VRI PDF dictionary of the PAdES signature. Every certificate present in this PDF dictionary shall be referenced by one of the aforementioned `AttributeObject` elements.

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 each `AttributeObject` child element of the `CRLs` child element in a `VRI` component shall contain a reference to one validation object containing one CRL present in one VRI PDF dictionary of the PAdES signature. Every CRL present in this PDF dictionary shall be referenced by one of the aforementioned `AttributeObject` elements.

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 each `AttributeObject` child element of the `OCSPs` child element in a `VRI` component shall contain a reference to one validation object containing one OCSP response present in one VRI PDF dictionary of the PAdES signature. Every OCSP response present in this PDF dictionary shall be referenced by one of the aforementioned `AttributeObject` elements.

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 the `TU` child element in a `VRI` component shall have as value the same date string as the date string present within the TU entry of VRI PDF dictionary of the PAdES signature.

For PAdES signatures specified in ETSI EN 319 142-1 [i.3] and ETSI EN 319 142-2 [i.4], clause 5 the `AttributeObject` child element of `TS` child element in one `VRI` component shall contain a reference to one validation object containing one time-stamp token present in the TU entry of VRI PDF dictionary of the PAdES signature.

A.29 DocTimeStamp

A.29.1 General

This element shall be used to report on the document time-stamp within a PDF document.

A.29.2 XML

The value of the document time-stamp shall be reported on in the `DocTimeStamp` element.

The `DocTimeStamp` element shall be of type `SATimestampType`.

A.29.3 PAdES

For every document time-stamp in the PDF document, the report shall contain a `DocTimeStamp` element.

The `TimeStampValue` shall contain the time of the time-stamp contained in the entry with key `Contents` of the document time-stamp dictionary.

The `AttributeObject` shall contain a reference to the validation object containing the time-stamp contained in the entry with key `Contents` of the document time-stamp dictionary.

NOTE: A document time-stamp can be signed or unsigned.

A.30 Reason

A.30.1 General

This element shall be used to report on the entry with key `Reason` in the Signature PDF dictionary.

A.30.2 XML

The entry with key `Reason` in the Signature PDF dictionary stamp shall be reported on in the `Reason` element.

The `Reason` element shall be of type `SAReasonType`.

```
<xs:complexType name="SAReasonType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="ReasonElement" type="xs:string"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

A.30.3 PAdES

The value within `ReasonElement` child shall be the same as the value of the entry with key `Reason` in the Signature PDF dictionary.

A.31 Name

A.31.1 General

This element shall be used to report on the entry with key `Name` in the Signature PDF dictionary.

A.31.2 XML

The entry with key `Name` in the Signature PDF dictionary stamp shall be reported on in the `Name` element.

The `Name` element shall be of type `SANameType`.

```
<xs:complexType name="SANameType">
    <xs:complexContent>
        <xs:extension base="vr:AttributeBaseType">
            <xs:sequence>
                <xs:element name="NameElement" type="xs:string"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

A.31.3 PAdES

The value within `NameElement` child shall be the same as the value of the entry with key `Name` in the Signature PDF dictionary.

A.32 ContactInfo

A.32.1 General

This element shall be used to report on the entry with key `ContactInfo` in the Signature PDF dictionary.

A.32.2 XML

The entry with key `ContactInfo` in the Signature PDF dictionary stamp shall be reported on in the `ContactInfo` element.

The `ContactInfo` element shall be of type `SAContactInfoType`.

```
    <xs:complexType name="SAContactInfoType">
        <xs:complexContent>
            <xs:extension base="vr:AttributeBaseType">
                <xs:sequence>
                    <xs:element name="ContactInfoElement" type="xs:string"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
```

A.32.3 PAdES

The value within `ContactInfoElement` child shall be the same as the value of the entry with key `ContactInfo` in the Signature PDF dictionary.

A.33 SubFilter

A.33.1 General

This element shall be used to report on the entry with key `SubFilter` in the Signature PDF dictionary.

A.33.2 XML

The entry with key `SubFilter` in the Signature PDF dictionary stamp shall be reported on in the `SubFilter` element.

The `SubFilter` element shall be of type `SASubFilterType`.

```
    <xs:complexType name="SASubFilterType">
        <xs:complexContent>
            <xs:extension base="vr:AttributeBaseType">
                <xs:sequence>
                    <xs:element name="SubFilterElement" type="xs:string"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
```

A.33.3 PAdES

The value within this component shall be the same as the value of the entry with key `SubFilter` in the Signature PDF dictionary.

EXAMPLE: Possible values are:

- ETSI.RFC3161
- ETSI.CAdES.detached
- adbe.pkcs7.detached
- adbe.pkcs7.sha1

A.34 ByteRange

A.34.1 General

This element shall be used to report on the entry with key `ByteRange` in the Signature PDF dictionary.

A.34.2 XML

The entry with key `ByteRange` in the Signature PDF dictionary stamp shall be reported on in the `ByteRange` element.

The `ByteRange` element shall be of type `SAListOfIntegers`.

This element shall consist in a list of integers whose number shall be multiple of two. Each group of two shall include the values of the two corresponding pair integers present in the entry with key ByteRange within Signature PDF dictionary. For each pair of integers in the list, the first one represents the starting byte offset. The second one represents the length of this range in bytes.

NOTE: The entry with key `ByteRange` may contain an array of pairs of integers.

A.34.3 PAdES

A PAdES signature signs the whole document and consequently has only one pair of integers in the `ByteRange` child.

The values within the `Range` child shall be the same integer values as the corresponding pair of integers present in the entry with key `ByteRange` in the Signature PDF dictionary.

A.35 Filter

A.35.1 General

This element shall be used to report on the entry with key `Filter` in the Signature PDF dictionary.

A.35.2 XML

The entry with key `Filter` in the Signature PDF dictionary stamp shall be reported on in the `Filter` element.

The `Filter` element shall be of type `SAFilterType`.

```
    <xs:complexType name="SAFilterType">
        <xs:sequence>
            <xs:element name="Filter" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
```

A.35.3 PAdES

The value within `Filter` child shall be the same as the value of the entry with key `Filter` in the Signature PDF dictionary.

Annex B (normative): XML Schema

The XML Schema file for the present document is in the file "TS119102-2-v111.xsd" contained in archive ts_11910202v010101p0.zip which accompanies the present document and is available at https://www.etsi.org/deliver/etsi_ts/119100_119199/11910202/01.01.01_60/.

History

Document history		
V1.1.1	August 2018	Publication