Draft ETSI TS 119 102-2 V0.1.2 (2017-11)

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

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 30 JANUARY 2018

Download the template for comments:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

Reference
DTS/ESI-0019102-2

Keywords
electronic signature, trust services signature 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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx.

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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.

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 multipart 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.

Introduction

Digital signatures are a major cornerstone for electronic commerce, provided they can be validated in such a way that participants have confidence in the fact that they answer their (business) needs. In this perspective, a participant may call a Trust Service Provider (TSP) that will perform the validation on his behalf. Such TSP is called a Signature Validation Service Provider (SVSP). The outcome of such service is a (or a series of) signature validation report(s).

The present document defines the elements of validation reports meeting the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.3]

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 [**Error! Reference source not found.**], ETSI EN 319 132-1 [9], ETSI EN 319 142-1 [10] respectively). This specification is aligned with the requirements specified in EN 319 102 part 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] EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

[2] OASIS DSS Profile for Comprehensive Multi-Signature Verification Reports Version 1.0

[3] D. Hühnlein, I. Henkel, J. C. Cruellas, S. Drees, A. Kuehne, et. al.: "DSS Verification Report Schema", July 2009, http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cd1.xsd

[4] D. Eastlake et al. "XML-Signature Syntax and Processing", W3C Recommendation, June 2008 (http://www.w3.org/TR/xmldsig-core/)

[5] ETSI: "XML Advanced Electronic Signatures (XAdES)", ETSI TS 101 903, Version 1.3.2, March 2006

[6] OASIS DSS Protocols, Elements and Bindings Version 1.0

[7] Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1 OASIS Standard, 2 September 2003

[8] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005

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

[10] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

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

[i.3] 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.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [1] and in ETSI TR 119 001 [i.4], and the following apply.:

signature augmentation: process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term

NOTE1: Augmenting signatures is a co-lateral process to the validation of signatures, namely the process by which certain material (e.g. time stamps, validation data and even archival-related material) is incorporated to the signatures for making them more resilient to change or for enlarging their longevity.

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

signature validation report: comprehensive report of the validation provided by the SVA to the DA and allowing the DA to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the SVA

NOTE: clause 5.1.3 of ETSI EN 319 102-1 [i.5] specifies minimum requirements for the content of such a report and ETSI TS 119 102-2 specifies 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

(signature) validation constraint: technical criteria against which a digital signature can be validated, e.g. as specified in EN 319 102-1

EXAMPLE: criteria can be expressed as an abstract formulation of rule, value, parameter, range and computation result

NOTE: validation constraints can be defined in a formal signature validation policy can be given in configuration parameter files or implied by the behaviour of the signature validation application.

….

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [2], in ETSI TR 119 001 [i.4] and the following apply:

DA: Driving Application

SD: Signer's Document

SDO: Signed Data Object

SVA: Signature Validation Application

4 Signature Validation Report Structure

4.1 Introduction

This document defines the structure of reporting the result of the validation of an AdES digital signature (specified in ETSI EN 319 122-1 [**Error! Reference source not found.**], ETSI EN 319 132-1 [**Error! Reference source not found.**], ETSI EN 319 142-1 [**Error! Reference source not found.**] respectively). The signature validation application (SVA) is assumed to follow the signature validation model specified in ETSI EN 319 102-1 [1] and illustrated by Figure 1.

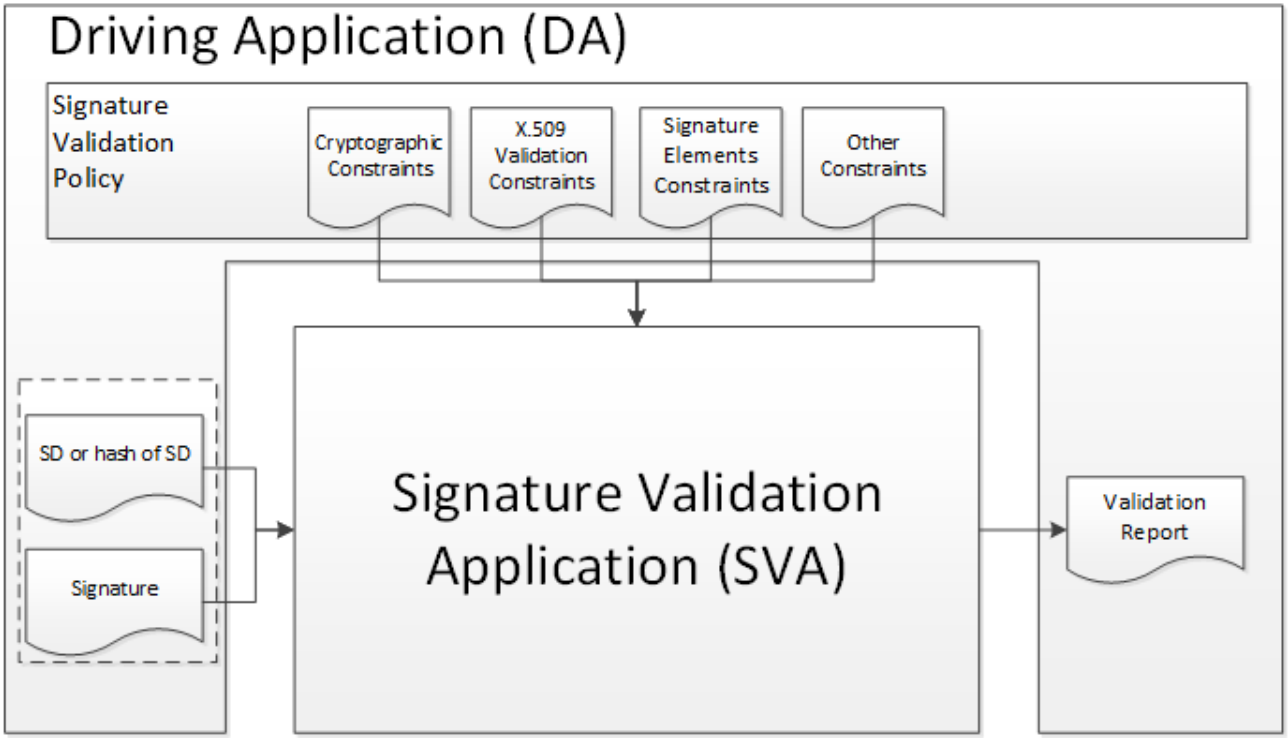

Figure 1: Conceptual Model of Signature Validation ETSI EN 319 102-1 [1]

The signature validation report shall consist of the following elements:

- One or more S*ignature validation report*-elements, containing the overall signature validation status for one or more signatures as well as general information on the signature validation performed. Clause 4.2 describes this element.
- A *signature validation objects*-element, containing objects used during validation, such as trust anchors, CRLs, or time-stamps. Clause 4.3 describes this element.

Signature validation report elements shall contain references to signature validation objects in the *signature validation objects*-element.

Figure 2 illustrates this structure. Figure 3 shows the structure with the elements contained in each of the fields.

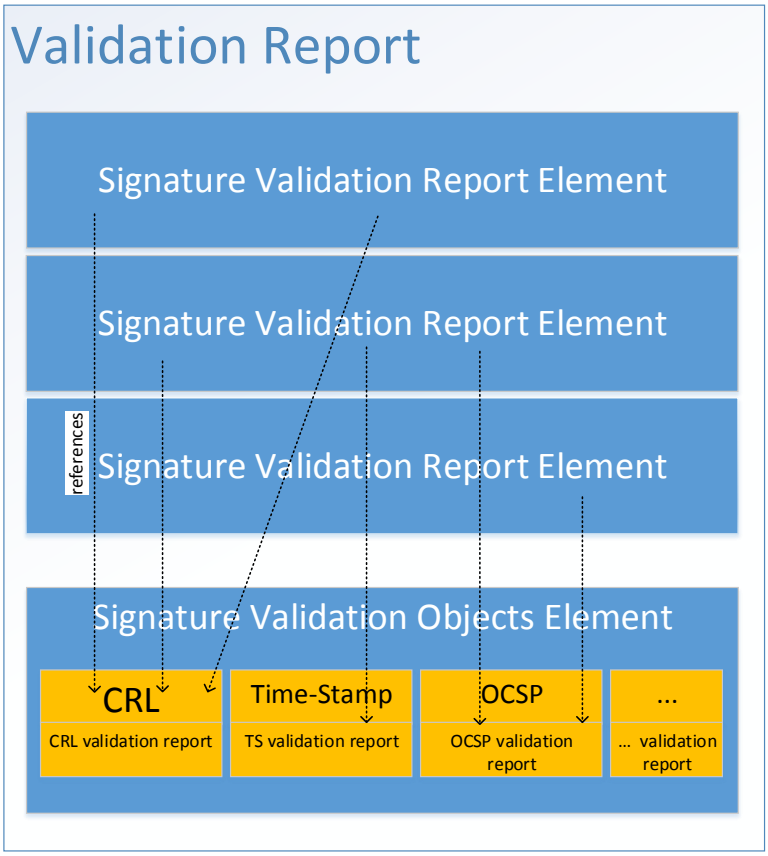

Figure 2: Signature Validation Report Structure

Element		
Validation Report	Signature Validation Report	Signature Identification Element Validator Information Signature Validation Status Indication Signature Validation Status Sub-Indication Formal Policy Policy Identifier Policy Name URLs Validation Constraint Validation Constraint Identifier Validation Constraint Status (Applied, Disabled, Overridden) Constraint Validation Result main status indication status sub-indication associated validation report data elements trust anchor certificate chain signed data objects

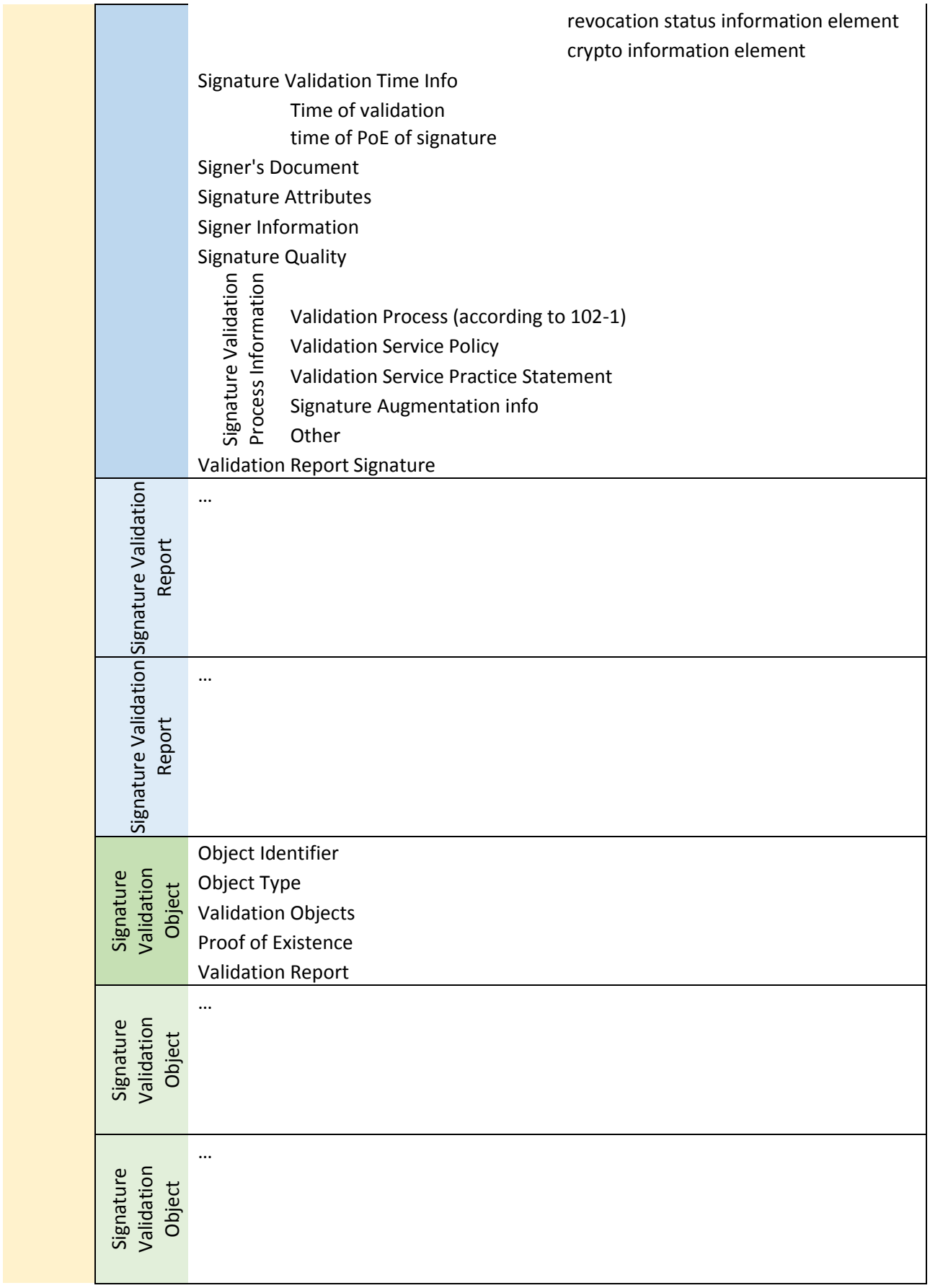

Figure 3: Validation Report Structure and Elements

4.2 Signature-Validation-Report-Element

4.2.1 General

The signature-validation-report-element contains information on the overall signature validation status as well as general information on the signature validation performed. A signature-validation-report-element corresponds to a single signature. Clause 4.2 defines the possible elements contained in the signature-validation-report-element.

4.2.2 Signature Identification Element

This element shall be present and shall identify the signature that has been the scope of the validation.

This element shall contain:

1) The DTBSR (see clause 4.2.8 in ETSI EN 319 102-1 [1]) together with an identifier of the hash algorithm used to calculate the hash;

This element may also contain one or more of the following

2) The digital signature value;

3) An identifier provided by the DA;

4) Other elements, which help identifying a signature and the signature data in a unique manner.

The element shall contain an indication whether the DTBSF (see clause 4.2.7 in ETSI EN 319 102-1[1]) or the DTBSR (see clause 4.2.8 in ETSI EN 319 102-1 [1]) has been seen by the SVA.

4.2.3 Validator Information

When present, this element shall contain information on the identity of the entity validating the signature and creating the validation report.

It shall provide at least one of the following identification information:

1) The digital identity of the validation service as used in a Trusted List, see TS 119 612 [i.2]

EXAMPLE: X.509 certificates, X.509 issuer distinguished name/serial number pair or X509 V.3 SubjectKeyIdentifiers.

2) a SAML identifier of type saml:NameIdentifierType [7] or saml:NameIDType [8]

3) Other information identifying the validator

4.2.4 Signature Validation Status Indication

4.2.4.1 General

This element shall be present and it shall contain the status on the full validation of the signature in the context of a particular signature validation policy.

The status indication provided shall contain the main status indication element as defined in 4.2.4.2.

The status indication may contain one or more sub-indication elements as defined in 4.2.4.3.

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

4.2.4.2 Main Status Indication Element

The main status indications shall be according to ETSI EN 319 102-1 [1], clause 5.1.3:

1) TOTAL-PASSED

2) TOTAL-FAILED or

3) INDETERMINATE

Different values or representations for these indications may be used. In this case the equivalence to the indications listed above shall be obvious to the user.

EXAMPLE: Different words, like VALID, or symbols like✓.

4.2.4.3 Status Sub-Indication Element

When the main status indication is *TOTAL-FAILED* or *INDETERMINATE,* this element shall be present, otherwise this element may be present.

The Status Sub-Indication element shall consist of

- A sub-indication that shall clearly identify the reason for the main status indication and
- optional associated validation report data elements (see clause **Error! Reference source not found.**) supporting that sub-indication.

There may be more than one sub-indication element present in a validation report. Sub-indications and associated validation report data (see clause **Error! Reference source not found.**12) should be according to ETSI EN 319 102-1 [1], clause 5.1.3, table 6.

4.2.5 Validation Constraints

4.2.5.1 General

This element shall be present and shall specify the set of validation constraints that have been driving the validation process, irrespective of the way the constraints have been defined (see ETSI EN 319 102-1 [1] clause 5.1.4.1).

Validation constraints shall be reported either

1) As a reference to a formal policy specification as specified in ETSI TS 119 172-1 [**Error! Reference source not found.**] when this formal policy specification has been selected explicitly or implicitly by the DA; or

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

2) As individual validation constraints.

A validation report may contain a reference formal policy specifications and individual constraints.

A validation report shall contain reports on validation constraints that have been applied implicitly by the SVA.

A validation report shall contain information on checks that a validation conformant to ETSI EN 319 102-1 [1] would require, but have been disabled by the policy or a validation constraint.

When a signature policy provided by the DA was not applied or not applied completely by the SVA, the validation report shall report on which constraints were applied and which ones have been ignored or overridden.

4.2.5.2 Formal Policy Element

When present, his element shall contain a signature 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

4.2.5.3 Validation Constraint Element

When present, this element shall indicate an individual signature validation constraint that has been applied during validation. It 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 so, by which one.

In addition, this element may contain:

1) The validation result for the constraint, when the validation of the constraint has not been disabled or overridden;

2) Any parameters the validation constraints requires;

3) 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 the length or the type of revocation checking required for the RevocationCheckingConstraints.

When present, the constraint validation result shall contain a main status indication (PASSED, FAILED, INDETERMINATE).

When present, the constraint validation result may contain

1) A sub-indication.

2) Additional associated validation report data elements (see clause **Error! Reference source not found.**)

4.2.6 Signature Validation Time Info

This element shall be present and 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.

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.

4.2.7 Signer’s Document Element

This element shall be present and shall identify the data that has been covered by the signature (DTBS). The DTBS consists of the Signer’s Data (SD) or the Signer's document representation (SDR) and the signature attributes selected to be signed together with the SD or SDR.

This element shall contain

1) The SDR and

2) A reference to a signature validation object within the Signature Validation Objects – Element (see clause 4.3) whenever the SD has been provided by the DA to the SVA. This object shall contain the SD.

4.2.8 Signature Attributes Element

This element shall be present whenever the signature contained signature attributes.

It shall consist of a list of all attributes contained in the signature together with the information whether the attribute was a signed or an unsigned attribute.

4.2.9 Signer Information Element

This element shall be present.

1) It shall contain a reference to an object in the Signature Validation Objects element (see clause 4.3). 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.

2) It may 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.

3) When a pseudonym has been used at the time of signing, it shall contain an element indicating whether that a pseudonym has been used at the time of signing; otherwise, it may contain such element.

4.2.10 Signature Quality Element

When present, this element shall contain information supporting the quality of the signature.

EXAMPLE: qualified electronic signature, advanced electronic signature supported by a qualified certificiate.

4.2.11 Signature Validation Process Information Element

This element shall be present and shall contain one or more of

1) An identifier indicating the validation process (see ETSI EN 319 102-1[1], clauses 5.3, 5.5, 5.6.3) that has been used in validation;

2) Information identifying the validation service policy, when applicable;

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

4) Information on augmentation of the signature, when applicable;

5) Other information provided by the SVP

4.2.12 Associated Validation Report Data Element

4.2.12.1 General

When present in a validation status sub-indication element, this element shall contain additional information on the validation of the signature or a signature validation constraint. It contains one or more of the elements described in the following subclauses.

All elements in the following subclauses may contain additional information.

4.2.12.2 Trust Anchor Element

This element shall identify the public key that has been used as the trust anchor in the validation process. It shall contain at least one of the following:

- The public key of the trust anchor
- An identifier referencing an object in the Signature Validation Objects element (see 4.3) that contains a certificate for public key of the trust anchor

This element shall be present when the main status indication is TOTAL-PASSED.

4.2.12.3 Certificate Chain Element

This element shall contain a list of identifiers referencing objects in the Signature Validation Objects element (see 4.3). This list shall contain the identifiers for the signing certificate (clause 4.2.9) as the first element and the trust anchor (4.2.12.2) and the last element. The certificates referenced by this list shall be the certificate chain used in the validation process.

4.2.12.4 Signed Data Objects Element

This element shall contain a list of references to signed data objects in the Signature Validation Objects element (see 4.3). This list shall not be an empty list.

NOTE: This list can contain one element only.

This element shall be used to relate a validation status sub-indication or a validation constraint sub-indication to the data objects that caused that sub-indication.

EXAMPLE: This element contains a list of references to timestamps when the validation sub-indication is TIMESTAMP_ORDER_FAILURE.

4.2.12.5 Revocation Status Information Element

This element shall be present when the main status indication is TOTAL_FAILED or INDETERMINATE and the status sub-indication is REVOKED resp. REVOKED_NO_POE or REVOKED_CA_NO_POE.

It shall contain

1) an identifier referencing a certificate in the Signature Validation Objects element (see 4.3)
2) the time of revocation
3) a reason for the revocation, and
4) an identifier referencing a CRL or OCSP response in the Signature Validation Objects element (see 4.3) that has been used for determining that revocation status

4.2.12.6 Crypto Information Element

This element shall be present when the main status indication is INDETERMINATE and the sub-indication is CRYPTO_CONSTRAINTS_FAILURE. This element shall contain

1) An identifier referencing an object in the Signature Validation Objects element (see 4.3);
2) An identifier referencing a cryptographic algorithm that has been used when producing the object; and
3) An identifier specifying whether the algorithm and the algorithm-parameters were considered secure or insecure.

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.

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

4.2.12.7 Additional Validation Report Data

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

1) An identifier identifying the type of additional information present
2) The additional information

NOTE: This element can be used for the sub-indication *GENERIC* [1].

4.2.13 Validation Report Signature

This element shall contain the signature over the signature validation report element and shall be created by the authority that performed the validation and created the validation report.

4.3 Signature Validation Objects

4.3.1 General

This element shall be present and it shall contain a list 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.

Clause 4.3 describes the properties of each element in this list.

4.3.2 Object Identifier

This property shall be present and shall contain an identifier that identifies the validation object uniquely within the validation report.

NOTE: This property can be used to refer to the validation object from the validation report.

4.3.3 Object Type

This property shall be present and shall uniquely identify the type of the validation object. It shall be represented by one of the following:

1) An ASN.1 identifier

2) A Mime-Type, or

3) An XML Schema Datatype

4.3.4 Validation Object

This property shall be present and shall contain a copy of or a reference to the validation object. How to incorporate the object into the report is format dependent; it shall be one of the following:

1) The object itself.

2) A Base64-encoded version of the object, or

3) A URI where the object can be retrieved together with a cryptographic hash of the object.

4.3.5 Proof of Existence (PoE)

This property shall contain the time for which a proof-of-existence for this object has been determined during validation. When the validation process determines multiple PoE-values for an object, this element shall contain the information on the PoE providing the earliest time for the existence of the object.

It shall contain the time value for that proof in UTC.

It may contain an identifier of the signature validation object that was essential for that proof.

NOTE: There is no signature validation object for deriving a proof when the PoE has been provided by the DA.

EXAMPLE: evidence records or time stamps.

4.3.6 Validation Object validation report

This property shall contain a validation report for the signature validation objects. This element shall be present whenever the signature validation object is a signed object and the signature has been validated during the overall validation.

This validation report shall conform to the present document, except that it shall not contain a Signature Validation Objects element and it shall not contain the Validation Report Signature element. Any 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.

5. XML-Format for Signature Validation Report

5.1 General

Clause 5 specifies how a signature validation report is to be represented in XML. The representation is based on the OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0 [2]. It maps the elements defined in clauses 4.2 and 4.3 to the elements defined in that profile and defines new elements where necessary.

Conventional XML namespace prefixes are used in the present document:

- The prefix `etsi-vr` (or no prefix) stands for the namespace for the present document.
- The prefix `vr:` stands for the OASIS-DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0 namespace [3].
- The prefix ds: stands for the W3C XML Signature namespace [4].
- The prefix xades: stands for ETSI XML Advanced Electronic Signatures (XAdES) document [5]
- The prefix dss: stands for the DSS core namespace [6].

A signature validation report may include other elements defined in [2] that are not mentioned in the present document.

5.2 Signature Validation Report Element

5.2.1 General

The Signature Validation Report Element as specified in clause 4.2 shall be of type `vr:IndividualReportType` element as specified in clause 3.3 of the OASIS profile [2].

5.2.2 Signature Identification Element

The Signature Identification Element as specified in clause 4.2.2 shall be the `<SignedObjectIdentifier>` element as specified in clause 3.3 of the OASIS profile [2]. It shall contain at least one of the following child-elements:

- To identify the signature by the DTBSR, the `XAdES:DigestAlgAndValue`-attribute;
- To identify the signature by the digital signature value, a `<ds:SignatureValue>`-element; and
- To identify the signature by an identifier or other elements, the `Other`-element.

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

5.2.2.1 `ValidationBasedOnHash` Element

If the validation is only based on the Data to be signed formatted (DTBSF) or Data to be signed representation (DTBSR), the `<Other>` element in the `SignedObjectIdentifier` element specified in clause 3.3 of the OASIS profile shall contain a `ValidationBasedOnHash` Element. This is defined as follows:

```
<element name="ValidationBasedOnHash" type="boolean" minOccurs="0" maxOccurs="1" />
```

5.2.3 Validator Information

The Validator Information as specified in clause 4.2.3 shall be of type `vr:IdentifierType`, as defined in clause 3.2 if the OASIS Profile [2].

NOTE The element is defined outside the `<IndividualReport>` element in OASIS since it is part of the protocol while here it is part of the validation report.

5.2.4 Signature Validation Status Indication

5.2.4.1 General

The signature validation status indication shall be provided as an element of type `vr:VerificationResultType`, as defined in clause 3.4 if the OASIS Profile [2].

5.2.4.2 Main Status Indication Element

The main status indication shall be expressed by the element vr:`ResultMajor` using the following URIs:

- *TOTAL-PASSED:* `urn:oasis:names:tc:dss:1.0:detail:valid`
- *TOTAL-FAILED* `urn:oasis:names:tc:dss:1.0:detail:invalid`
- *INDETERMINATE* `urn:oasis:names:tc:dss:1.0:detail:indetermined`

5.2.4.3 Status Sub-Indication Element

The sub-indication shall be expressed by the element vr:`ResultMinor` and 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_FAIL URE
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
GENERIC	urn.etsi.019102.subindication.GENERIC

The status indication should contain associated validation report data as specified in tables 5 and 6 of [1] as associated validation data elements as specified in clauses 5.2.12

5.2.5 Validation Constraints

5.2.5.1 General

Information on the validation constraints that were applied during validation shall be placed in the `<vr:Details>` element within `<vr:IndividualSignatureReport>` and shall be contained in an element of type `ValidationConstraintsType`, defined as follows:

```
<complexType name=”ValidationConstraintsType”>
    <sequence>
        <element ref=”XAdES:SignaturePolicyIdentifier” maxOccurs=”1” minOccurs=”0” />
        <element name=”ValidationConstraint” type=”SingleValidationConstraintType” minOccurs=”0”
maxOccurs=”unbounded” />
    </sequence>
</complexType>
```

It may contain the following elements:

`<XAdES:SignaturePolicyIdentifier>` [Optional]

When present, the element shall contain an identifier of the signature validation policy defining the set of constraints that have been applied during validation.

`<ValidationConstraint>` [Optional]

When present, the element shall contain a single validation constraint that has been applied, disabled or overridden during validation of the signature. It shall be of type `SingleValidationConstraintType` defined in 5.2.5.1.

5.2.5.2 SingleValidationConstraint Type

This type specifies a single validation constraint. It shall be contained in an element of type `SingleValidationConstraintType` defined as follows:

```
    <xs:complexType name="SingleValidationConstraintType">
        <xs:sequence>
            <xs:element name="ValidationConstraintIdentifier" type="xs:anyURI" minOccurs="1"/>
            <xs:element name="ValidationConstraintParameter"
                    type=" etsi-vi:ValidationConstraintParameterType" minOccurs="0"
                    maxOccurs="unbounded"/>
            <xs:element name=”ConstraintStatus” type=”etsi-vr:ConstraintStatusType” minOccurs=”1”
                    maxOccurs=”1”>
            <xs:element name="VerificationResult" type="vr:VerificationResultType"
                        minOccurs=”0” />
            <xs:element name="Hint" type="xs:anyType">:
        </xs:sequence>
```

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

This element shall contain

1) a URI that uniquely identifies the validation constraint in the element `ValidationConstraintIdentifier`.

2) an element of type `ConstraintStatus` defined in 5.2.5.3. and

3) the result of validating this constraint as an element of type `vr:VerificationResultType`, whenever the `ConstraintStatus` has the value applied.

The element may contain one or more parameters of type `ValidationConstraintParameterType` defined in 5.2.5.2.

5.2.5.3 ValidationConstraintParameter Type

This type specifies a parameter that has been used when validating a single validation constraint. It contains a parameter type and a parameter value and is defined as follows:

```
    <xs:complexType name="ValidationConstraintParameterType">
        <xs:sequence>
            <xs:element name="ParameterType" type="xs:anyURI"/>
            <xs:element name="ParameterValue" type="xs:anyType"/>
        </xs:sequence>
    </xs:complexType>
```

5.2.5.4 ConstraintStatus Type

This type is used to declare whether a constraint has been applied, disabled or overridden.. It is defined as follows:

```
    <xs:complexType name="ConstraintStatusType">
        <xs:sequence>
            <xs:element name="Status" type="xs:anyURI" minOccurs="1"/>
            <xs:element name="OverriddenBy" type="xs:anyType" minOccurs="0"/>
            <xs:element name="Indications" type="xs:anyType" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
```

The `Status`-element shall contain one of these identifiers:

1) `urn.etsi.019102.constraintStatus.applied`

2) `urn.etsi.019102.constraintStatus.disabled`

3) `urn.etsi.019102.constraintStatus.overridden`

When the `Status`-element contains the indication that the constraint has been overridden, the element `OverriddenBy` shall contain a reference to the corresponding constraint.

Indications for steps to be taken to potentially get a determinate result, when the main status indication is INDETERMINATE, shall be put in the `Indications`-element.

5.2.6 Signature Validation Time Info

This element shall be of type `dss:VerificationTimeInfoType`. It shall be placed in the `<dss:Details>` element within `<dss:IndividualSignatureReport>` and contain

- The date and time the validation was performed in the `<VerificationTime>` element as specified in [2].
- The date and time for which the existence of the signature can be proven and the validation status has been determined in a `<AdditionalTimeInfo>` element of type `urn.etsi.019102.bestSignatureTime`, its value shall be of type `xs:dateTime`.

All values shall be expressed as UTC time (Coordinated Universal Time).

5.2.7 Signer's Document

The signers document element shall be represented as an element of type `etsi-vr:SignersDocumentType`. It shall be placed in the `<dss:Details>` element within `<dss:IndividualSignatureReport>`. This element shall consist of:

- The SDR in an element of type `XAdES:DigestAlgAndValueType`.
- The reference to the signer's document in an element of type `etsi-vr:VOReferenceType`.

```
    <xs:complexType name="SignersDocumentType">
        <xs:sequence>
            <xs:element name="DigestAlgAndValue"
                type="XAdES:DigestAlgAndValueType" maxOccurs="1" minOccurs="0"/>
            <xs:element name="SignersDocument" type="VOReferenceType" minOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
```

5.2.8 Signature Attributes

Signed and unsigned signature attributes shall be contained in an element of type `vr:PropertiesType a`s specified in clause 3.5.4 of the OASIS profile [2].

5.2.9 Signer Information

The signer information shall be contained in an element of type `etsi-vr:SignerInformationType`. It shall be placed in the `<dss:Details>` element within `<dss:IndividualSignatureReport>`. This element shall contain the reference to the signer's certificate in an element of type `etsi-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 `etsi-vr:Pseudonym` attribute indicating this.

```
    <xs:complexType name=" SignerInformationType">
        <xs:sequence>
            <xs:element name="SignerCertificate" type="VOReferenceType" minOccurs="1" />
            <xs:element name="Signer" type="string" />
            <xs:element name="SignerInfo" type="dss:AnyType" minOccurs="0" />
        </xs:sequence>
        <attribute name="Pseudonym" type=boolean" use="optional" />
    </xs:complexType>
```

5.2.10 Signature Quality Element

The signature quality information shall be contained in an element of type `etsi-vr:SignatureQualitytype`. It shall be placed in the `<dss:Details>` element within `<dss:IndividualSignatureReport>`. It shall contain a list of identifiers that specify the quality of the signature determined during validation.

```
<xs:complexType name=" SignatureQualitytype ">
    <xs:element name="SignatureQalityInformation" type="anyURI" minOccurs="0"/>
 </xs:complexType>
```

5.2.11 Signature Validation Process Info

This optional element shall be of type `SignatureValidationProcessType`. It shall be placed in the `<dss:Details>` element within `<dss:IndividualSignatureReport>` and is defined as follows:

```
    <xs:complexType name="SignatureValidationProcessType">
        <xs:sequence>
            <xs:element name="SignatureValidationProcessID" type="anyURI" />
            <xs:element name="SignatureValidationServicePolicy" type="anyURI" minOccurs="0"/>
            <xs:element name="SignatureValidationPracticeStatement" type="anyURI" minOccurs="0"/>
            <xs:element name="AugmentationInfo" type="xs:anyType" minOccurs="1"/>
            <xs:element name="Other" type="xs:anyType" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
```

The element SignatureValidationProcessID shall contain an identifier that 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 EN 319 102-1 clause 5.3.
- urn.etsi.019102.validationprocess.LTV when the SVA performed the Validation Process for Signatures with Time and Signatures with LongTerm- Validation Material as specified in ETSI EN 319 102-1 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 EN 319 102-1 clause 5.6.

When present, the element SignatureValidationServicePolicy shall contain a URI identifying the validation service policy.

When present, the element AugmentationInfo shall provide information on any augmentation performed after validation of the signature.

When present, the element Other shall contain any other information about the validation process provided by the SVA.

5.2.12 Associated Validation Report Data

5.2.12.1 General

Associated Validation Report Data shall be provided in the <dss:Details> element within <dss:IndividualSignatureReport> in an element of Type ValidationReportDataType that is defined as follows:

```
<xs:complexType name="ValidationReportDataType">
    <xs:sequence>
        <xs:element name="SigningCertificate" type="VOReferenceType" maxOccurs="1"/>
        <xs:element name="CertificateChain" type="VOReferenceType" maxOccurs="1"/>
        <xs:element name="SignedDataObjects" type="VOReferenceType" maxOccurs="1"/>
        <xs:element name="RevocationStatusInformation" type="RevocationStatusInformationType"/>
        <xs:element name="CryptoInformation" type="CryptoInformationType" />
        <xs:element name="AdditionalValidationReportData"
            type="AdditionalValidationReportDataType" />
    </xs:sequence>
</xs:complexType>
```

Where VOReferenceType is used to reference validation objects within the validation report and is defined as follows:

```
<xs:complexType name="VOReferenceType">
    <xs:attribute name="VOReference" type="xs:IDREFS" use="required"/>
</xs:complexType>
```

.

5.2.12.2 Trust Anchor Element

This element shall 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.

5.2.12.3 Certificate Chain Element

This element shall be of type VOReferenceType and shall contain a list of identifiers of objects in the Signature Validation Objects element. The first element of the list shall be the identifier of the signing certificate (clause 5.1.7.1) and the last element of the list shall be the trust anchor (5.1.7.2). The certificates referenced by this list shall form the certificate chain used in the validation process.

5.2.12.4 Signed Data Objects Element

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

5.2.12.5 Revocation Status Information Element

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

```
    <xs:complexType name="RevocationStatusInformationType">
        <xs:sequence>
            <xs:element name="ValidationObjectId" type="VOReferenceType" minOccurs="1"/>
            <xs:element name="RevocationTime" type="xs:dateTime"/>
            <xs:element name="RevocationReason" type="anyURI" minOccurs="0" maxOccurs=”1”/>
            <xs:element name="RevocationObject" type="VOReferenceType" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
```

The element `ValidationObjectId` shall contain an identifier referencing 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. The following URIs shall be used:

```
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:unspecified
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:keyCompromise
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:cACompromise
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:affiliationChanged
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:superseded
urn:oasis:names:tc:dssx:1.0:profiles:verificationreport:revocationreason:cessationOfOperation
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:certificateHold
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:removeFromCRL
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:privilegeWithdrawn
urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:revocationreason:aACompromise
```

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.

5.2.12.6 Crypto Information Element

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

```
    <xs:complexType name="AlgorithmParameterType">
        <xs:sequence>
            <xs:element name="ParameterID" type="xs:anyURI" minOccurs="1" maxOccurs="1" />
            <xs:element name="Value" type="xs:anyType" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="CryptoInformationType">
        <xs:sequence>
            <xs:element name="ValidationObjectId" type="VOReferenceType" minOccurs="1"/>
            <xs:element name="Algorithm" type="xs:anyURI" minOccurs="1"/>
            <xs:element name="AlgorithmParameters" type="AlgorithmParameterType" minOccurs="0"/>
            <xs:element name="NotAfter" type="xs:dateTime" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
```

The element `ValidationObjectId` shall contain an identifier referencing a signed object in the Signature Validation Objects element. The element `Algorithm` shall contain a URI that identifies the algorithm. The element `AlgorithmParameters` shall specify algorithm-specific parameters that have been used. The element `NotAfter` shall contain the time when the algorithm or parameter was no longer considered secure.

5.2.12.7 Additional Validation Report Data

This element shall be of type `AdditionalValidationReportData`Type 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="ReportDataType">
        <xs:sequence>
            <xs:element name="InfoType" type="xs:anyURI" minOccurs="1" maxOccurs="1"/>
            <xs:element name="InfoData" type="xs:anyType" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="AdditionalValidationReportDataType">
        <xs:sequence>
            <xs:element name="ReportData" type="ReportDataType" minOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
```

5.2.13 Validation Report Signature

A XAdES signature as defined in ETSI EN 319 132 1 [9] or ETSI EN 319 132 2 [10] shall be placed in the `<dss:Details>` element within `<dss:IndividualSignatureReport>` and shall cover the whole validation report including the signature validation objects.

5.3 Signature Validation Objects

The signature validation objects shall be placed in the `<dss:Details>` element within `<dss:IndividualSignatureReport>` and shall be contained in an element of type `ValidationObjectListType` and shall be defined as follows:

```
    <xs:complexType name="PoEType">
        <xs:sequence>
                <xs:element name="PoETime" type="xs:dateTime" minOccurs="1" maxOccurs="1"/>
                <xs:element name="PoEObject" type="VOReferenceType" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

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

    <xs:complexType name="ValidationObjectType">
        <xs:sequence>
            <xs:element name="ObjectType" type="xs:anyURI"/>
            <xs:element name="ValidationObject" type="ValidationObjectRepresentationType"/>
            <xs:element name="PoE" type="PoEType" minOccurs="0"/>
            <xs:choice minOccurs="0" maxOccurs="1">
                <xs:element name="ValidationReport" type="vr:IndividualReportType"/>
                <xs:element ref="vr:IndividualTimeStampReport"/>
                <xs:element ref="vr:IndividualCertificateReport"/>
                <xs:element ref="vr:IndividualAttributeCertificateReport"/>
                <xs:element ref="vr:IndividualCRLReport"/>
                <xs:element ref="vr:IndividualOCSPReport"/>
                <xs:element ref="vr:EvidenceRecordReport"/>
            </xs:choice>
        </xs:sequence>
        <xs:attribute name="id" type="xs:ID" use="required"/>
    </xs:complexType>

    <xs:complexType name="ValidationObjectRepresentationType">
        <xs:choice>
            <xs:element name="direct" type="xs:anyType"/>
            <xs:element name="base64" type="xs:base64Binary"/>
            <xs:element name="URI" type="xs:anyURI"/>
        </xs:choice>
    </xs:complexType>
```

To specify the type of revocation 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.other
```

The validation report of the validation object shall be of type `individualReportType` when the validation of the signature of the validation object required the use of the Validation Process for Signatures with Time and Signatures with LongTerm- Validation Material or the Validation process for Signatures providing Long Term Availability and Integrity of Validation Material.

Annex (informative): Change History

Date	Version	Information about changes
05 17	0.0.1	First draft for STF 524
06 17	0.1.0	First draft for ESI #59
11 17	0.1.1	Draft in preparation to Steering Group
11 17	0.1.2	Draft for public review