Draft ETSI TS 119 172-4 V0.0.7 (2019-08)

Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists

Reference
DTS/ESI-0019172-4

Keywords
electronic signature, e-commerce,
trust services

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
http://portal.etsi.org/tb/status/status.asp

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

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
Introduction 4
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definition of terms, symbols, abbreviations and notations 8
3.1 Terms 8
3.2 Symbols 8
3.3 Abbreviations 8
3.4 Notations 8
4 Signature applicability rules for the validation of EU qualified electronic signatures/seals 8
4.1 Introduction 8
4.2 Validation constraints and validation procedures 9
4.3 Requirements on signature validation and applicability rules checking practices 10
4.4 Technical applicability (rules) checking process 10
4.4.1 Overview 10
4.4.2 Processing 10
4.5 Requirements on applicability rules checking report 12
History 14

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 4 of a multi-part deliverable specifying Signature Policies as identified below:

Part 1: "Building blocks and table of contents for human readable signature policy documents";

Part 2: "XML Format for signature policies";

Part 3: "ASN.1 Format for signature policies";

Part 4: "Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

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

A digital signature is always used in a context, either implicit or explicit, e.g. as part of a business process.

Regulation (EU) No 910/2014 [i.1] defines the terms electronic signature, advanced electronic signature, qualified electronic signature, electronic seal, advanced electronic seal and qualified electronic seal. These electronic signatures and seals can be created using digital signature technology.

NOTE 1: When not stated otherwise in the present document, "signature" denotes "digital signature".

The purpose of signature applicability rules is to describe the requirements imposed on or committing the involved actors (signers, verifiers, relying parties and/or potentially one or more trust service providers) with respect to the applicability of signatures to documents and data that are signed in a particular context, transaction, process, business or application domain, in order to determine whether these signatures are fit for a particular business or legal purpose.

NOTE 2: The terms "signature applicability rules" are known as "signature validation policy" in ETSI TS 119 172-1 [4] while they are being used in other standards like ETSI TS 119 102-1 [1], ETSI TS 119 441 [i.10] to identify the "*set of rules, applicable to one or more digital signatures, that defines the requirements for their determination of whether a signature is fit for a particular business or legal purpose*". The terms "signature validation policy" is used in these latter documents to refer to a very specific set of technical constraints to technically validate a digital signature. Signature applicability rules can include more rules than those applying to those technical signature validation constraints. ETSI TS 119 172-1 [4] can be used to define such signature applicability rules.

EXAMPLE: An example of such applicability is the determination whether a digital signature can be determined as an EU qualified electronic signature or seal in accordance with (EU) No 910/2014 [i.1], in particular with its Art.32 on "Requirements for the validation of qualified electronic signatures" where the term validation is understood in the common sense. In this context the "applicability rules" adds, to the technical validation of the signature, verification that the signer certificate has been issued as an EU qualified certificate for electronic signature/seal, that it was a valid qualified certificate at the time of signing, that the signature creation data resides in a qualified electronic signature/seal creation device, etc.

There needs to be some way of expressing the rules for the technical validation of digital signatures and the determination of their applicability to the specific context of Article 32 of the eIDAS Regulation, i.e. to determine whether they can be (technically) considered as European qualified electronic signatures/seals using trusted lists (TLs) in the sense of the applicable European legislation at the time of signing, i.e. either Directive 1999/93/EC [i.2] or Regulation (EU) No 910/2014 [i.1].

The present document specifies such rules.

1 Scope

The present document specifies a set of rules that aims at defining the technical requirements for determining, taking into account the EU Member States trusted lists [i.4], whether a digital signature is fit for meeting the requirements of EU qualified electronic signatures/seals in the sense of the applicable European legislation, i.e. either Directive 1999/93/EC [i.2] or Regulation (EU) No 910/2014 [i.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 EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Signature Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[2] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[3] ETSI TS 119 612 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[4] ETSI TS 119 172-1: "Electronic Signature Infrastructure; Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

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

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

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

[8] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[9] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[10] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[11] ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

[12] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[13] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[14] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[15] Recommendation ITU-T X.520 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[16] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[17] ETSI TS 119 615: "Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists".

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

[i.2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.3] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures; Definitions and abbreviations".

[i.4] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.5] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.6] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.7] ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

[i.8] OJ C 233, 28.6.2016, p. 1–5: Information related to data on Member States' trusted lists as notified under Commission Decision 2009/767/EC, as amended by Decision 2010/425/EU and Implementing Decision 2013/662/EU and as notified under Implementing Decision (EU) 2015/1505.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG

[i.9] ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".

[i.10] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

[i.11] ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 441 [i.10] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.3] and the following apply:

CRL	Certificate Revocation List
CV	Cryptographic Verification
EU	European Union
OCSP	Online Certificate Status Protocol
QSCD	Qualified Signature/seal Creation Device
SSCD	Secure Signature Creation Device
TARC	Technical Applicability (Rules) Checking
TL	Trusted List

3.4 Notations

The requirements in the present document are identified as follows:

<REQ> - <the clause number> - <2-digit number - incremental>

The management of the requirement identifiers for subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2-digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for deleted requirements are kept and completed with "VOID".
- The requirement identifier for modified requirement are kept void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 Signature applicability rules for the validation of EU qualified electronic signatures/seals

4.1 Introduction

The requirements defined by the present document are organised in terms of:

a) Requirements on the validation constraints and validation procedures in the sense of ETSI TS 119 102-1 [1],

b) Requirements on signature validation and applicability rules checking practices;

c) Requirements on the process of checking technical applicability (rules);

d) Requirements on reporting the results of the applicability rules checking.

4.2 Validation constraints and validation procedures

REQ-4.2-01: The driving application or the signature validation application shall follow the validation process, as specified in ETSI EN 319 102-1 [1], clause 5.1.2 and shall support the Validation process for Signatures providing Long Term Availability and Integrity of Validation Material.

REQ-4.2-01bis: The present document gives the minimum requirements for QES as in the Regulation:

a) The validation service may use additional inputs or additional requirements.

b) If additional inputs are used, they shall be clearly indicated.

REQ-4.2-02: The constraints to be used as input to the validation process referred to in REQ-4.2-01 shall be as follows:

X.509 validation constraints

a) The SetOfTrustAnchors constraint defined in ETSI TS 119 172-1 [4], clause A.4.2.1, table A.2 rows (m)1.1 shall be set to the relevant information from the 'Service digital identity' field(s) from the `SI-Results` output of the procedure specified in clause 4.3 of ETSI TS 119 615 [17], considering as input

i) the signing certificate, as successfully identified as per the execution of clause 5.2.3 of ETSI TS 119 102-1 [1] as part of step 2 of clause 5.3.4 of [1],

ii) the value http://uri.etsi.org/TrstSvc/Svctype/CA/QC for the TLS-Sti Service type identifier, and

iii) the NotBeforeDate value of the signing certificate for the Date-time indication.

NOTE 1: The use of the `NotBeforeDate` value of the signing certificate here above is expected to identify the date at which the certificate has been issued as a valid (qualified) certificate, even if technically it can have been created before that date.

NOTE 2: The validation of any time-stamp does not require that the corresponding trust anchor is defined as a time-stamping generation service within an EU Member State national TL. See also REQ-4.5-01.d).ii).

b) Constraints defined in ETSI TS 119 172-1 [4], clause A.4.2.1, table A.2 rows (m)1.2 to (m)1.10 shall not be used.

c): With regards to revocation constraints:

i) The RevocationCheckingConstraints shall be set to "eitherCheck" as defined in ETSI TS 119 172-1 [4], clause A.4.2.1, table A.2 rows (m)2.1.

iv) Constraint defined in ETSI TS 119 172-1 [4], clause A.4.2.1, table A.2 rows (m)2.2 and (m).3 shall not be used.

ii) Constraint defined in ETSI TS 119 172-1 [4], clause A.4.2.1, table A.2 rows (m)2.3 shall be used.

Cryptograhic constraints

NOTE 3: Guidance on cryptographic algorithms validity can be found in ETSI TS 119 312 [i.6].

d) The cryptographic verification process specififed in ETSI TS 119 102-1 [1] shall enable the validation procedure to report the relying party with information related to cryptographic suites used to generate the signature being validated and potential security related issues against either national rules or ETSI TS 119 312 [i.6], indicating clearly which of the national rules or ETSI TS 119 312 [i.6] has been used to express potential security issues.

e) When the signature validation application is not able to deal with a specific algorithm or cryptographic suite, it shall not invalidate the signature for that reason but lead to an INDETERMINATE result and raise a warning indicating the concerned cryptographic suite and the fact it is not supported.

Signature elements constraints

f) Failure to comply with one of the signature formats identified in REQ-4.3-01 shall not result in invalidating the signature but in a warning indicating such a failure and the reasons for such a failure.

4.3 Requirements on signature validation and applicability rules checking practices

NOTE 1: The requirements of the present section refers to the practices whose related statements are referred to ETSI TS 119 172-1 [4], clause A.2.

REQ-4.3-01: The signature validation application should support signature formats compliant with :

a) ETSI TS 103171 [8],

b) ETSI TS 103172 [9],

c) ETSI TS 103173 [10],

d) ETSI TS 103174 [11], and

e) ETSI standards on baseline profiles for CAdES digital signatures (ETSI EN 319 122-1 [5]), XAdES digital signatures (ETSI EN 319 132-1 [6]), and PAdES digital signatures (ETSI EN 319 142-1 [7]).

NOTE 2: This aims to support CID (EU) 2015/1506 [i.5].

REQ-4.3-02: Signature validation applications should be compliant with ETSI TS 119 101 [i.7].

REQ-4.3-03: When provided as a service, the validation and applicability rules checking processes should be provided in compliance with ETSI TS 119 441 [i.10].

REQ-4.3-04: Relying parties shall be provided with unambiguous information with regards to any security relevant issue identified by the signature validation and applicability rules checking processes.

REQ-4.3-05: Relying parties shall be provided with procedures and facilities to validate the signatures and obtain validation and applicability rules checking results data.

REQ-4.3-06: Relying parties shall be provided with procedures and facilities allowing them to identify the relevance of further actions to be taken when the preservation of signed data and associated signatures is required.

NOTE 2: Guidance on preservation of signed data and associated signatures can be found in ETSI TS 119 511 [i.11].

4.4 Technical applicability (rules) checking process

4.4.1 Overview

The present section defines a process for implementing technical applicability (rules) checks aiming to facilitate the determination whether a digital signature can be considered technically suitable to implement EU qualified electronic signatures/seals using trusted lists in the sense of the applicable European legislation at the time of signing, i.e. either Directive 1999/93/EC [i.2] or Regulation (EU) No 910/2014 [i.1].

This process aims to support the "validation" process referred to in Article 32(1) of Regulation (EU) No 910/2014 [i.1].

The inputs of this process are the outputs of the process performed as specified in clause 4.2 of the present document and the main output is a status indicating the technical suitability of the digital signature to implement an EU qualified electronic signature or seal in the sense of Article 32 of Regulation (EU) No 910/2014 [i.1].

4.4.2 Processing

NOTE 1: The next two requirements aim to support the verification of point (a) of Article 32(1), respectively Article 40, of [i.1].

REQ-4.4.2-01: The technical applicability (rules) checking (TARC) process shall perform the process specified in clause 4.4 of ETSI TS 119 615 [17], with `CERT` set to the signing certificate and `Date-time` set to the best signature time resulting from the process performed as specified in REQ-4.2-01.

REQ-4.4.2-02: When, as a result of REQ-4.4.2-001, `QC-Status` include the value "PROCESS_PASSED" and `QC-Results` include either "QC_For_eSig" or "QC_For_eSeal":

a) then, the signing certificate shall be technically determined, at the signing time being estimated at `Date-time`, respectively as an EU qualified certificate for electronic signatures or an EU qualified certificate for electronic seals;

b) otherwise:

(i) the process stops;

(ii) the signature shall be technically determined as indeterminate, i.e. neither an EU qualified electronic signature, nor as an EU qualified electronic seal; and

(iii) the above result and the results of processes of all the intermediate processes shall be reflected in the signature applicability rules checking report.

NOTE 2: The next three requirements aim to support the verification of point (b) of Article 32(1), respectively Article 40, of [i.1].

NOTE 3: The next two requirements aim to support the verification of points (c), (d), and (e) of Article 32(1), respectively Article 40, of [i.1].

REQ-4.4.2-03: If any of the checks specified in REQ-4.4.2-03 fails, then:

a) the process stops;

b) the signature shall be technically determined as indeterminate, i.e. as neither an EU qualified electronic signature, nor as an EU qualified electronic seal; and

c) the above result and the results of processes of all the intermediate processes shall be reflected in the signature applicability rules checking report.

NOTE 4: The next two requirements aim to support the verification of point (f) of Article 32(1), respectively Article 40, of [i.1].

REQ-4.4.2-04: The TARC process shall perform the process specified in clause 4.5 of ETSI TS 119 615 [17], with `CERT` set to the signing certificate and `Date-time` set to the best signature time resulting from the process performed as specified in clause 4.2 of the present document.

REQ-4.4.2-05: When, as a result of REQ-4.4.2-04, `QSCD-Status` include the value "PROCESS_PASSED" and `QSCD-Results` include "QSCD_YES":

a) then, the digital signature shall be technically determined, at the best signature time, as having been created by a qualified signature/seal creation device;

b) otherwise:

(i) the process stops;

(ii) the signature shall be technically determined as inderterminate, i.e. neither an EU qualified electronic signature, nor as an EU qualified electronic seal; and

(iii) the above result and the results of processes of all the intermediate processes shall be reflected in the signature applicability rules checking report.

NOTE 5: Requirements of points (g) and (h) of Article 32(1) of [i.1] are expected to be met when the result of the signature validation procedure performed against ETSI EN 319 102-1 [1] as specified in clause 4.2 or against any equivalent purpose procedure leads to respectively TOTAL-PASSED [1] or any equivalent result, with regards to the best signature time.

REQ-4.4.2-06: At that point of the TARC process, if the following conditions are met:

a) the signing certificate is determined, at the best signature time, as an EU qualified certificate for electronic signatures (respectively for electronic seals), as specififed in REQ-4.4.2-002 a);

b) the digital signature is determined, at the best signature time, as having been created by a qualified signature (respectively seal) creation device, as specififed in REQ-4.4.2-005 a); and

c) the result of the process performed as specified in clause 4.2 of the present document is *TOTAL-PASSED*.

then the digital signature shall be determined as technically suitable to implement an EU qualified electronic signature (respectively an EU qualified electronic seal), otherwise the signature shall not be determined technically either as an EU qualified electronic signature, or as an EU qualified electronic seal.

4.5 Requirements on applicability rules checking report

NOTE 1: REQ-4.5-01 aims to support the implementation of Art.32.2 of the eIDAS Regulation [i.1]. It can be structured using ETSI TS 119 102-2 [i.9].

REQ-4.5-01 The signature applicability rules checking report shall include the following elements that shall be presented in a way that is meaningful to the verifier when this verifier is a natural person:

a) The following text on the scope of the applicability rules checking (validation in the sense of [i.1]) executed on the validated signature:

> ***Signature applicability rules checking (validation rules) for European qualified electronic signatures/seals using trusted lists***
>
> *Validation of digital signature to identify whether it can be considered technically suitable to implement a European qualified electronic signature/seal using EUMS trusted lists in the sense of the applicable European legislation at the time of signing, i.e. either Directive 1999/93/EC or Regulation (EU) No 910/2014;*
>
> EDITORIAL NOTE: Add an URI to identify the present signature applicability rules (and inherent validation policy).

b) The complete set of data representing the signer in its certificate, including the data available in the `Subject` field of the signing certificate and, when present, the data available in its `Subject Alternative Name` extension [3].

c) The use of any pseudonym is clearly indicated if a pseudonym was used at the best signature time;

d) The time reference against which the results of the signature applicability rules checking shall be provided as follows:

i) The absence of the corresponding trust anchor from an EU Member State TL (i.e. 'Service type identifier' http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST or http://uri.etsi.org/TrstSvc/Svctype/TSA) should be expressed via an information in the validation report.

> NOTE 2: Clause 4.3 of ETSI TS 119 615 [17] can be used to obtain for a certificate, for a 'Service type identifier' and for a specific date and time, a matching trust anchor service and its associated service information from an EU Member Sate TL.

ii) The signature applicability rules checking report shall indicate, whenever applicable, the following timing information:

1) claimed signing time,
2) time of the document time-stamp / time assertion,
3) time of the signature time-stamp / time assertion,
4) time of revocation (or suspension) of the signer's certificate,
5) time of OCSP response / time of CRL issuance & next update, at least for the signer's certificate,
6) the best signature time.

iii) For each of the indicated timing information from the list provided in point ii) above, the report shall indicate, whenever applicable, their evidential relevance and their level of assurance, including when applicable [12]:

1) The policy identifier for the time-stamping policy used by the time-stamping authority;
2) The accuracy of the time-stamp;
3) The indication whether the time-stamp is qualified under Regulation (EU) 910/2014 [i.1] or not;

> NOTE 3: Clause 4.6 of ETSI TS 119 615 [17] can be used to determine whether a time stamp token is confirmed by the applicable EUMS trusted list to have been an EU qualified time stamp.

EXAMPLE: With regard to time-stamps, it addresses whether the time-stamping authorities issuing time stamps used in this context are trust service providers known and trusted by the relying party and the level of quality/security/accuracy of the time-stamping policy.

e) The presentation of the data that is covered by the signature (i.e. signed data);

NOTE 3: It is important that the relying party is provided with unambiguous information on what data has been actually signed by the signer.

f) Any signature attributes that have been included in the signature and an indication of which attributes were signed and which were not signed;

NOTE 4: This covers intention to sign, intention to seal and the potential expression of the commitment expressed alongside the signature, either implicitly or explicitly (e.g. through commitment types) [4].

g) The overall status of the signature applicability rules checking, and the reasons having led to such a result.

NOTE 5: ETSI EN 319 102-1 [1] specifies such status and reasons.

h) Information related to cryptographic suites used to generate the signature being validated and potential security related issues against either national rules or ETSI TS 119 312 [i.6]. It shall indicate clearly which of the national rules or ETSI TS 119 312 [i.6] failed when expressing potential security issues; and

i) Optionally, the detailed outcome of each step of the signature applicability rules checking, including those of the technical signature validation.

History

Document history		
0.0.1	04/08/2015	Initial draft version (as TS 119 172-4, was previously drafted in TS 119 172-1)
0.0.2	01/06/2016	Updated draft.
0.0.3	27.02.2017	Stable draft.
0.0.4	12.06.2017	Final draft.
0.0.5	06.02.2018	Final draft.
0.0.6	20.03.2019	Final draft.
0.0.7	05.08.2019	Updated draft from comments at ESI#67.