ETSI TS 119 403-2 V1.2.4 (2020-11)

Electronic Signatures and Infrastructures (ESI);
Trust Service Provider Conformity Assessment;
Part 2: Additional requirements for
Conformity Assessment Bodies auditing Trust Service
Providers that issue Publicly-Trusted Certificates

Reference
RTS/ESI-0019403-2v124

Keywords
conformity, e-commerce, electronic signature,
security, 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

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 Trust Service Provider Conformity Assessment, as identified below:

ETSI EN 319 403-1:	"Requirements for conformity assessment bodies assessing Trust Service Providers";
ETSI TS 119 403-2:	**"Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates";**
ETSI TS 119 403-3:	"Additional requirements for conformity assessment bodies assessing EU qualified trust service providers".

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

ISO/IEC 17065 [i.6] is an international standard which specifies general requirements for conformity assessment bodies (CABs) performing certification of products, processes, or services. These requirements are not focused on any specific application domain where CABs work.

In ETSI EN 319 403-1 [1] the general requirements of ISO/IEC 17065 [i.6] are supplemented to provide additional dedicated requirements for CABs performing certification of trust service providers (TSPs) and the trust services they provide towards defined criteria against which they claim conformance.

ETSI EN 319 403-1 [1] aims to meet the general needs of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.1]. Its aims include support of national accreditation bodies (NABs) as specified in Regulation (EC) No. 765/2008 [i.2] in applying ISO/IEC 17065 [i.6] for the accreditation of CABs that certify TSPs and the trust services they provide so that this is carried out in a consistent manner. In accordance with EC Regulation No 765/2008 [i.2], attestations issued by conformity assessment bodies accredited by a NAB can be formally recognized across Europe. ETSI EN 319 403-1 [1] supplements ISO/IEC 17065 [i.6] by specifying additional requirements, e.g. on resources, on the assessment process and on the audit of a TSP's management system, as defined in ISO/IEC 17021 [i.4] and in ISO/IEC 27006 [i.5].

The present document specifies supplementary requirements to those defined in ETSI EN 319 403-1 [1] in order to provide additional dedicated requirements for CABs performing audits based on ETSI EN 319 411-1 [i.9] and those from CA/Browser Forum, [i.7] and [i.8].

1 Scope

The present document defines specific supplementary requirements to those defined in ETSI EN 319 403-1 [1] for CABs performing audits based on ETSI EN 319 411-1 [i.9] and those from CA/Browser Forum, [i.7] and [i.8].

In particular, the present document defines the requirements for audit attestations, including their content.

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 319 403-1 (V2.3.1) (06-2020): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

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.

NOTE: Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[i.2] EC Regulation No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

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

[i.4] ISO/IEC 17021: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems".

[i.5] ISO/IEC 27006: "Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems".

[i.6] ISO/IEC 17065: "Conformity assessment -- Requirements for bodies certifying products, processes and services".

[i.7] CA/Browser Forum (V1.7): "Guidelines for The Issuance and Management of Extended Validation Certificates".

[i.8] CA/Browser Forum (V1.7): "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

[i.9] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".

[i.10] ISO 8601-1:2019: "Date and time Part 1: Basic rules".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

Publicly-Trusted Certificate (PTC): certificate trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software

NOTE: 1: See ETSI EN 319 411-1 [i.9].

NOTE: 2: Within the context of the present document, PTC is used synonymously with EVC, DVC, IVC and OVC as per CA/B Forum documents [i.7] and [i.8]. The purpose of PTC is described in BRG [i.8], clause 1.4.1.

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:

AAL	Audit Attestation Letter
CA/B Forum	Certification Authority and Browser Forum
CAB	Conformity Assessment Body
PTC	Publicly-Trusted Certificate

4 Requirements for CABs auditing TSPs that issue PTCs

4.1 General

PTA-4.1-01: The requirements defined in ETSI EN 319 403-1 [1] shall apply.

The following clauses define additional requirements.

4.2 Audit Frequency (see ETSI EN 319 403-1, clause 7.4.5)

PTA-4.2-01: A full-surveillance audit shall be conducted no less frequently than annually.

PTA-4.2.02: Updated audit information shall be provided no less frequently than annually.

PTA-4.2.03: Successive audits shall include an evaluation of evidence produced since the last audit.

4.3 Audit Attestation

PTA-4.3-01: The Audit Attestation for TSPs issuing publicly-trusted certificates shall provide sufficient details to demonstrate that the audited TSP fulfilled the requirements from ETSI EN 319 411-1 [i.9] and those from CA/Browser Forum, [i.7] and [i.8].

In particular:

- PTA-4.3-02: The Audit Attestation shall be written in English.
- PTA-4.3-03: The Audit Attestation shall be in a "text searchable" PDF format.
- PTA-4.3-04: The Audit Attestation shall be uploaded to their auditor's website.
- PTA-4.3-05: The audit attestation Audit Attestation shall list the date on which the audit letter was written.
- PTA-4.3-05a: The Date Format shall use one of the following options:
  - YYYY-MM-DD example: 2016-05-07.

NOTE 1: This format is conformant with ISO 8601-1 [i.10]

- PTA-4.3-05b The date of the issuance of the audit attestation shall be not later than 90 days after the end of the audit period.
- PTA-4.3-06: The Audit Attestation shall have the CAB's name in the audit letter as well as the CAB's address, the CAB's contact information and information about the CAB's accreditation.
- PTA-4.3-07: The Audit Attestation shall be issued annually.
- PTA-4.3-08: The Audit Attestation shall include a statement on each sub-clause of the referenced requirements where there is a finding of nonconformity noted during the audit.

NOTE 2: With regards to PTA-4.3-08, pending non-conformities are only acceptable in line with clause 7.6 b) of ETSI EN 319 403-1 [1].

- PTA-4.3-09: The Audit Attestation shall include a clear identification of the audited TSP.
- PTA-4.3-10: The Audit Attestation shall list the full name, SHA256 thumbprints of the CA certificates of the TSP services that have been audited, and the applied policies of the audited TSP.
- PTA-4.3-10a: The Hash values of the SHA 256 thumbprints within the Audit Attestation shall not contain colons, spaces, line feeds, lower case letters or page break code.
- PTA-4.3-11: The Audit Attestation for a period of time audit shall state the start and end dates of the period that was audited (see PTA-4.3-05a).
- PTA-4.3-11a: The Audit Attestation for a point in time audit shall state the date of the point in time of the audit (see PTA-4.3-05a).
- PTA-4.3-12: The Audit Attestation shall list the audit standards that were used during the audit and list the full name and version of the audit standards referenced.
- PTA-4.3-13: The Audit Attestation shall list the policy and practice statement documents of the TSP that the audit was based on.
- PTA-4.3-14: The Audit Attestation shall list the city, state/province (if applicable), and country of all relevant physical locations used in Certification Authority operations.

NOTE 3: Root programs relying on audits based on ETSI EN 319 403-1 [1] and the present document may place additional requirements on the audit attestations for TSPs issuing publicly-trusted certificates.

4.4 Audit Scope

PTA-4.4-01: The audit attestation shall list all TSP incidents documented in a public repository (e.g. Mozilla® Bugtracker) with an explanation of remediation status.

NOTE: If the audit scope includes third party trust service components, such as a Registration Services as defined in ETSI EN 319 411-1 [i.9] the TSP remains responsible for this component and the component is addressed by the TSP's audit as in ETSI EN 319 403-1 [1], clause 7.4.1.0.

Annex A (informative): Bibliography

- ENISA: "Guidelines on supervision of qualified trust services; Technical guidelines on trust services", December 2017. (update under preparation)
- ENISA: "Towards global acceptance of eIDAS audits", January 2019.
- ENISA: "Assessment of ETSI TS 119 403-3 related to eIDAS", November 2019.

NOTE: Available at https://www.enisa.europa.eu/publications.

Annex B (informative): Change History

Date	Version	Information about changes
July 2018	1.1.1	First publication of the TS after approval ETSI ESI #62.
April 2019	1.2.1	Included Change Requests: CR#1 "report non-conformities": see PTA-4.3-08 agreed at ESI#64
October 2020	1.2.1	Included Change Requests: CR#1 "Add a statement about RA Audits": Change of PTA-4.4.01 an add a Note CR#2 "Defining coding rules for the audit dates in AAL": see PTA-4.3-05a CR#3 "Delete statement about findings of critical non-conformities": see PTA-4.3-08 CR#4 "Defining Rules for encoding Hash Values": see PTA-4.3-10a CR#5 "New requirements for a point in time audit": see PTA-4.3-11a CR6# "List all CA incidents documented in a public repository" see PTA-4.4-01

History

Document history		
V1.1.1	July 2018	Publication
V1.2.1	April 2019	Publication
V1.2.4	November 2020	Publication