ETSI TS 119 403-3 V1.1.1 (2019-03)

Electronic Signatures and Infrastructures (ESI);
Trust Service Provider Conformity Assessment;
Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

Reference
DTS/ESI-0019403-3

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

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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 3 of a multi-part deliverable covering Trust Service Provider Conformity Assessment, as identified below:

Part 1: "Requirements for conformity assessment bodies assessing Trust Service Providers" (now existing as ETSI EN 319 403 to be issued as Part 1 when revised);

Part 2: "Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates";

Part 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.30] is an international standard which specifies general requirements for conformity assessment bodies (CABs) performing certification of products, processes, or services. These requirements are not focussed on any specific application domain where CABs work.

In ETSI EN 319 403 [1], the general requirements of [i.30] 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] 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], and from CA/Browser Forum [i.4]. It aims include support of national accreditation bodies (NABs) as specified in Regulation (EC) No. 765/2008 [i.3] in applying ISO/IEC 17065 [i.30] 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 [i.3], attestations issued by conformity assessment bodies accredited by a NAB can be formally recognized across Europe.
ETSI EN 319 403 [1] supplements ISO/IEC 17065 [i.30] 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 17021-1 [i.6] and in ISO/IEC 27006 [i.7].

The present document specifies supplementary requirements to those defined in [1] in order to provide additional dedicated requirements for CABs performing certification of qualified trust service providers (QTSPs) and the qualified trust services (QTSs) they provide towards the requirements of Regulation (EU) No 910/2014 [i.1]. It aims supporting NABs for the accreditation of CABs in line with Article 3.18 of Regulation (EU) No 910/2014 [i.1].

The ENISA technical guidelines on trust services "Guidelines on initiation of qualified trust services" [i.9] have been used as basis for the present document.

1 Scope

The present document defines specific supplementary requirements for the application of ETSI EN 319 403 [1] aimed at conformity assessments (audits) of qualified trust service providers (QTSPs) and the qualified trust services (QTSs) they provide, as well as of trust service providers, without qualified status, intending to start providing qualified trust services, against the requirements of Regulation (EU) No 910/2014 [i.1] assuming the use of ETSI policy requirement standards but not precluding use of other specifications.

In particular, the present document defines requirements for conformity assessment reports, 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: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

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

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

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

[i.2] 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.

NOTE: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D1505.

[i.3] 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.4] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[i.5] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.6] ISO/IEC 17021-1: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements".

[i.7] ISO/IEC 27006: "Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems".

[i.8] Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services.

NOTE: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2015.128.01.0013.01.ENG.

[i.9] ENISA: "Guidelines on initiation of qualified trust services; Technical guidelines on trust services", December 2017. ISBN: 978-92-9204-189-2.

NOTE: https://www.enisa.europa.eu/publications/tsp-initiation.

[i.10] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.11] 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.12] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.13] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[i.14] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[i.15] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".

[i.16] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.17] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.18] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.19] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

[i.20] ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services".

[i.21] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.22] 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.23] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists".

[i.24] 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 unsigned data using signature techniques".

[i.25] ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques".

[i.26] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.27] ETSI EN 319 522 (all parts): "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services".

[i.28] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.29] ETSI EN 319 532 (all parts): "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services".

[i.30] ISO/IEC 17065: "Conformity assessment -- Requirements for bodies certifying products, processes and services".

[i.31] CEN EN 419 221-5: "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services".

[i.32] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements for Trustworthy Systems Supporting Server Signing".

[i.33] CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing".

[i.34] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

[i.35] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

[i.36] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.5] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.5] and the following apply:

CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CID	Commission Implementing Decision
HSM	Hardware Security Module
NAB	National Accreditation Body
PEM	Privacy-Enhanced electronic Mail
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
SB	Supervisory Body

3.4 Notations

The requirements in the present document are identified as follows:

<3 letters identifying the section title> **-** <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-digits 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 Requirements for CABs assessing QTSP/QTSs against requirements of Regulation (EU) No 910/2014

4.1 Conformity assessment scheme

CAS-4.1-01: The conformity assessment scheme for which a CAB is accredited to assess QTSP/QTSs against the requirements of Regulation (EU) No 910/2014 [i.1] in accordance with Regulation (EC) No 765/2008 [i.3] shall be defined in a way that such accreditation ensures the accredited CAB is competent to carry out conformity assessment of a QTSP/QTS against the requirements of Regulation (EU) No 910/2014 [i.1].

In particular:

CAS-4.1-02: The conformity assessment scheme shall, with the aim of confirming that the assessed QTSP/QTS fulfils the applicable requirements from Regulation (EU) No 910/2014 [i.1], include:

a) requirements on the CAB, including on the auditing rules under which the CAB will carry out its conformity assessment and on the effective set of criteria, meeting at least requirements from ETSI EN 319 403 [1]; and

NOTE: This de facto implies the CAB being compliant with ETSI EN 319 403 [1], hence with ISO/IEC 17065 [i.30], to be a certification body and the conformity assessment scheme to be a certification scheme [i.30].

b) control objectives and controls against which the CAB will assess a QTSP/QTS against the applicable requirements of Regulation (EU) No 910/2014 [i.1].