SLOVENSKI STANDARD
oSIST prEN 319 403-1 V2.3.0:2020

01-februar-2020

Elektronski podpisi in infrastruktura (ESI) - Ugotavljanje skladnosti ponudnikov storitev zaupanja - 1. del: Zahteve za ugotavljanje skladnosti organov, ki ocenjujejo ponudnike storitev zaupanja

Electronic Signatures and Infrastructures (ESI) - Trust Service Provider Conformity Assessment - Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers

Ta slovenski standard je istoveten z: **ETSI EN 319 403-1 V2.3.0 (2019-11)**

__ICS:__

03.080.99	Druge storitve	Other services
35.040.01	Kodiranje informacij na splošno	Information coding in general

oSIST prEN 319 403-1 V2.3.0:2020   **en**

iTeh STANDARD PREVIEW

(standards.iteh.ai)

Draft ETSI EN 319 403-1 V2.3.0 (2019-11)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI);
Trust Service Provider Conformity Assessment;
Part 1: Requirements for conformity assessment bodies
assessing Trust Service Providers

Reference
REN/ESI-0019403v231

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

Copyright Notification

ETSI

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 draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

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 [1] 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 the present document the general requirements 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.

The present document is aiming to meet the general requirements 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.10].

The present document's aims include support of national accreditation bodies as specified in Regulation (EC) No. 765/2008 [i.4] in applying ISO/IEC 17065 [1] 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.4], attestations issued by conformity assessment bodies accredited by a national accreditation body can be formally recognized across Europe.

The present document does not repeat requirements from ISO/IEC 17065 [1] but follows its document structure. Where needed, additional requirements are specified. This is mainly the case for requirements on resources (clause 6) and on the assessment process (clause 7). For all other chapters of ISO/IEC 17065 [1] few or no additional requirements are needed.

The present document also incorporates many requirements relating to the audit of a TSP's management system, as defined in ISO/IEC 17021 [i.12] and in ISO/IEC 27006 [i.11]. These requirements are incorporated by including text to derived from these documents in the present document, as well indirectly through references to requirements of ISO/IEC 17021 [i.12].

1　　Scope

The present document contains requirements for the competence, consistent operation and impartiality of conformity assessment bodies assessing and certifying the conformity of Trust Service Providers (TSPs) and the trust services they provide towards defined criteria against which they claim conformance.

NOTE 1:　Those requirements are independent of the type and class of trust service provided.

The present document also contains requirements for the conformity assessment of trust services component services, which later forms part of a separate conformity assessment of a TSP.

NOTE 2:　This enables a provider of such component services, which are used as part of the service provided by several TSPs, to avoid having to be assessed several times, or even for a TSP to provide a service based just on a component service or collection of components whether or not they are recognized as a trust service under Regulation (EU) No 910/2014 [i.1].

The present document applies the general requirements of ISO/IEC 17065 [1] to the specific requirements of conformity assessment of TSPs.

The present document is part 1 of a multipart standard. Other parts include:

- ETSI TS 119 403-2 [i.14]: 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.

- ETSI TS 119 403-3 [i.15]: Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers.

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

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 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2]   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.3]   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.4]   Regulation (EC) 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.5]   ISO/IEC 17000:2004: "Conformity assessment -- Vocabulary and general principles".

[i.6]   ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.7]   ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.8]   ISO/IEC 27001: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.9]   ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.10]   CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

[i.11]   ISO/IEC 27006: "Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems".

[i.12]   ISO/IEC 17021: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems".

[i.13]   ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security controls".

[i.14]   ETSI TS 119 403-2: "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".

[i.15]   ETSI TS 119 403-3: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers".

[i.16]   ETSI TS 119 431 (all parts): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers".

3   Definition of terms, symbols and abbreviations

3.1   Terms

For the purposes of the present document, the terms given in ISO/IEC 17065 [1] and the following apply:

auditor: person who assesses conformity to requirements as specified in a given requirements document

competence: ability to apply knowledge and skills to achieve intended results

conformity assessment: process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled

NOTE: From Regulation (EC) No 765/2008 [i.4] and section 2.1 of ISO/IEC 17000:2004 [i.5].

conformity assessment body: body that performs conformity assessment services which is accredited as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides

NOTE: This is equivalent to conformity assessment body as specified in point 13 Article 2 of Regulation (EC) No 765/2008 [i.4].

minor nonconformity: non-fulfilment of a specified requirement that does not have any major security impact, and does not have any major impact on the ability of the TSP to meet the intended service

national accreditation body: sole body in a State that performs accreditation with authority derived from the State

NOTE: This is equivalent to national accreditation body as specified in point 11 Article 2 of Regulation (EC) No 765/2008 [i.4].

technical expert: person who provides specific knowledge or expertise to the audit team

NOTE 1: Specific knowledge or expertise relates to the organization, the process or activity to be audited, or language or culture.

NOTE 2: A technical expert does not act as an auditor in the audit team.

trust service: electronic service which enhances trust and confidence in electronic transactions

NOTE: Such trust services typically, but not necessarily, use cryptographic techniques or manipulate confidential material.

trust service component: one part of the overall service of a TSP

NOTE 1: A typical example of such component services are those identified in clause 4.4 of ETSI EN 319 411-1 [i.2]. Also, ETSI TS 119 431 [i.16] defines requirements for a Server Signing Application Service Component (SSASC) which can be implemented as part of TSP's service which also includes other service components.

NOTE 2: Other standards, including ETSI standards, can also specify requirements for other service components which can form part of a wider TSP's service.

Trust Service Provider (TSP): entity which provides one or more electronic trust services

3.2   Symbols

Void.

3.3   Abbreviations

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

CA   Certification Authority
CAB   Conformity Assessment Body
EC   European Commission
EU   European Union
IT   Information Technology
TSP   Trust Service Provider

4   General requirements

4.1   Legal and contractual matters

4.1.1   Legal responsibility

The requirements from ISO/IEC 17065 [1], clause 4.1.1 shall apply.

4.1.2   Certification agreement

The requirements from ISO/IEC 17065 [1], clause 4.1.2 shall apply.

4.1.3   Use of license, certificates and marks of conformity

The requirements from ISO/IEC 17065 [1], clause 4.1.3 shall apply.

4.2   Management of impartiality

4.2.0   General requirements

The requirements from ISO/IEC 17065 [1], clause 4.2 shall apply. In addition, the following TSP-specific requirements and guidance apply.

4.2.1   Activities not conflicting with impartiality

Conformity Assessment Bodies and its personnel may carry out additional activities provided they do not constitute a risk to its impartiality. These activities may include but are not limited to:

a)   organizing and participating in information meetings about the certification scheme in general;

b)   arranging and participating as a lecturer in training courses, provided that, where these courses relate to TSPs, related security controls or auditing, lecturers shall confine themselves to the provision of generic information and advice which is publicly available;

c)   activities prior to audit, solely aimed at determining readiness for audit; however, such activities shall not result in the provision of recommendations or advice for specific solutions and shall not result in a reduction in the eventual audit duration;

d)   performing third party audits according to standards, publicly available specifications or regulatory requirements other than those being part of the scope of accreditation; or

e)   adding value during audits.

EXAMPLE: Adding value during audits includes identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions.

4.3   Liability and financing

The requirements from ISO/IEC 17065 [1], clause 4.3 shall apply.

4.4   Non-discriminatory conditions

The requirements from ISO/IEC 17065 [1], clause 4.4 shall apply.