ETSI TS 119 403 V2.2.1 (2015-08)

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

Reference
RTS/ESI-0019403-TSv221

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 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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 8
4 General requirements 8
4.1 Legal and contractual matters 8
4.1.1 Legal responsibility 8
4.1.2 Certification agreement 8
4.1.3 Use of license, certificates and marks of conformity 8
4.2 Management of impartiality 8
4.2.0 General requirements 8
4.2.1 Activities not conflicting with impartiality 8
4.3 Liability and financing 8
4.4 Non-discriminatory conditions 9
4.5 Confidentiality 9
4.6 Publicly available information 9
5 Structural requirements 9
5.1 Organizational structure and top management 9
5.2 Mechanism for safeguarding impartiality 9
6 Resource requirements 9
6.1 Conformity Assessment Body personnel 9
6.1.1 General 9
6.1.2 Management of competence for personnel involved in the audit process 9
6.1.2.0 General requirements 9
6.1.2.1 Management of competence 9
6.1.2.2 Training of audit teams 9
6.2 Resources for evaluation 10
6.2.0 General requirements 10
6.2.1 Internal resources 10
6.2.1.0 General requirement 10
6.2.1.1 Competence of Conformity Assessment Body personnel 10
6.2.1.2 Competences for all functions 10
6.2.1.3 Competences for application review 10
6.2.1.4 Competences and prerequisites for auditing 11
6.2.1.5 Competences for review 11
6.2.1.6 Competences for certification decision 11
6.2.1.7 Competences for Technical Experts 11
6.2.1.8 Audit team 12
6.2.1.9 Audit team leader 12
7 Process requirements 13
7.1 General requirements 13
7.2 Application 13
7.3 Application Review 13
7.3.0 General requirements 13
7.4 Audit 13

7.4.0 General requirements 13
7.4.1 Audit Scope 13
7.4.1.0 Audit Scope General 13
7.4.1.1 Audit Team Mandate 14
7.4.1.2 Audit Methodology 14
7.4.2 Audit time 15
7.4.3 Multiple sites 15
7.4.3.1 When to Consider Sample Based Approach 15
7.4.3.2 Requirements of Sample Based Approach 15
7.4.4 Audit Report 16
7.4.4.1 Report contents 16
7.4.4.2 Report contents details to be provided 16
7.4.5 Audit process 17
7.4.5.1 General preparation for the initial audit 17
7.4.5.2 Audit Process 17
7.4.5.3 Stage 1 audit 17
7.4.5.4 Stage 2 audit 18
7.4.6 Audit Frequency 19
7.5 Review 19
7.6 Certification decision 19
7.7 Certification documentation 19
7.8 Directory of certified products 19
7.9 Surveillance 19
7.10 Changes affecting certification 20
7.11 Termination, reduction, suspension or withdrawal of certification 20
7.12 Records 20
7.13 Complaints and appeals 20
8 Management system requirements 21
8.1 Options 21
8.2 General management system documentation 21
8.3 Control of documents 21
8.4 Control of records 21
8.5 Management review 21
8.6 Internal audits 21
8.7 Corrective actions 21
8.8 Preventive actions 21
Annex A (informative): Auditors' code of conduct 22
Annex B (informative): Bibliography 23
History 24

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 (http://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).

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]. In particular this relates to the information security management system (ISMS), as defined 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 conformity of trust service providers (TSPs) and the trust services they provide towards defined criteria against which they claim conformance.

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

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

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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://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 reference 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 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: Policy requirements for certification authorities issuing qualified certificates".

[i.4] 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.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 supporting Electronic Signatures".