Final draft ETSI EN 319 403 V2.2.0 (2015-06)

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

Reference
REN/ESI-0019403

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

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 final draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the 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):	18 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]. 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 for Trust Service Providers issuing certificates".

[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 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".

[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 providing Time-Stamping Services".

[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".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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].

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 are typically but not necessarily using cryptographic techniques or involving confidential material.

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

3.2 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
ISMS	Information Security Management System
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.

4.5 Confidentiality

The requirements from ISO/IEC 17065 [1], clause 4.5 shall apply.

4.6 Publicly available information

The requirements from ISO/IEC 17065 [1], clause 4.6 shall apply.

5 Structural requirements

5.1 Organizational structure and top management

The requirements from ISO/IEC 17065 [1], clause 5.1 shall apply.

5.2 Mechanism for safeguarding impartiality

The requirements from ISO/IEC 17065 [1], clause 5.2 shall apply.

6 Resource requirements

6.1 Conformity Assessment Body personnel

6.1.1 General

The requirements from ISO/IEC 17065 [1], clause 6.1.1 shall apply.

6.1.2 Management of competence for personnel involved in the audit process

6.1.2.0 General requirements

The requirements from ISO/IEC 17065 [1], clause 6.1.2 shall apply. In addition, the following TSP-specific requirements and guidance apply.

6.1.2.1 Management of competence

The performance of the following functions as defined in clause 7 of ISO/IEC 17065 [1] shall need specific competences with respect to Trust Service Provider as described in clause 6.2:

a) application review;

b) audit;

c) review; and

d) certification decision.

6.1.2.2 Training of audit teams

The Conformity Assessment Body shall have criteria for the training of audit teams that support the ability to demonstrate competence in:

a) knowledge of the TSP standards and other relevant publicly available specifications;

b) understanding of trust services and information security including network security issues;

c) understanding of risk assessment and risk management from the business perspective;

d) technical knowledge of the activity to be audited;

e) general knowledge of regulatory requirements relevant to TSPs; and

f) knowledge of security policies and controls.

6.2 Resources for evaluation

6.2.0 General requirements

The requirements from ISO/IEC 17065 [1], clause 6.2 shall apply.

6.2.1 Internal resources

6.2.1.0 General requirement

The requirements from ISO/IEC 17065 [1], clause 6.2.1 shall apply. In addition, the following TSP-specific requirements and guidance apply.

6.2.1.1 Competence of Conformity Assessment Body personnel

The Conformity Assessment Body shall have personnel competent to:

a) select and verify the competence of TSP auditors for audit teams appropriate for the audit;

b) brief TSP auditors and arrange any necessary training;

c) decide on the granting, maintaining, withdrawing, suspending, extending, or reducing of certifications; and

d) set up and operate an appeals and complaints process.

6.2.1.2 Competences for all functions

The Conformity Assessment Body personnel shall have knowledge of:

a) standards and publicly available specifications relevant to TSP conformity assessment;

b) TSPs general concepts and relevant requirements;

c) TSPs' legal and regulatory requirements;

d) trust services functioning, and information security management including network security;

e) TSPs' security policies and controls; and

f) TSPs' risk assessment and risk management.

6.2.1.3 Competences for application review

The Conformity Assessment Body personnel reviewing TSPs' applications shall have the following specific competences:

a) technological and legal understanding of the areas of activity of the TSP and the associated business risks;

b) technical understanding of the evaluation process;

c) understanding of the competences and capabilities of the Conformity Assessment Body; and

d) communication and analytic skills to explain certification requirements to the client and to resolve possible difference in understanding regarding standards, other publicly available specifications or regulatory requirements.

6.2.1.4 Competences and prerequisites for auditing

The Conformity Assessment Body personnel performing audit as described in clause 7.4 shall have the following specific competences and knowledge, and fulfil the following requirements:

a) Requirements:

1) formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below; and

2) at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security, and physical security.Knowledge of:

1) audit principles, practices and techniques in the field of TSP audit gained in a training course of at least five days;

2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security;

3) the applicable standards, publicly available specifications and regulatory requirements for TSPs and other relevant publicly available specifications including standards for IT product evaluation; and

EXAMPLE: Applicable standards such as ISO/IEC 27002 [i.13], ETSI EN 319 401 [i.6], ETSI EN 319 411-1 [i.2], ETSI EN 319 411-2 [i.3], ETSI EN 319 421 [i.9] or ISO/IEC 15408 [i.7].

4) the Conformity Assessment Body's processes.

c) Competences:

1) language skills appropriate for all organizational levels within the TSP organization;

2) note-taking, report-writing, presentation, and interviewing skills; and

3) personal attributes: objective, mature, discerning, analytical, persistent and realistic.

The Conformity Assessment Body personnel performing audit shall maintain competence on the basis of appropriate education, training or experience. All relevant experience shall be current and prior to assuming responsibility for performing as an auditor, the candidate shall have gained experience in the entire process of TSP audit. This experience shall have been gained by participation under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting.

6.2.1.5 Competences for review

The Conformity Assessment Body personnel performing assessment information and results reviews shall have the specific competences described in clause 6.2.1.4 and have acted as auditor in, at least, three complete TSP assessments.

6.2.1.6 Competences for certification decision

The Conformity Assessment Body personnel performing assessment information and results revisions shall have the competences described in clause 6.2.1.2 and knowledge of certification process.

6.2.1.7 Competences for Technical Experts

Technical experts assisting the audit team provide specific knowledge or expertise during the audit process.

NOTE 1: Technical experts are not considered as auditors and do not need to have the complete auditor competences as described in clause 6.2.1.4.

Technical experts shall, at all times, be responsible to the audit team leader.

NOTE 2: Typical knowledge provided by technical experts includes the following:

a) knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of TSP and information security;

b) knowledge of the current technical state-of-art regarding Public Key Infrastructure;

c) knowledge in technologies applicable to the TSP trust service being audited;

d) knowledge of performing information security related risk assessments so as to identify TSP assets, threats and vulnerabilities providing understanding of their occurrence, impact and their mitigation;

e) knowledge of network security vulnerability analysis including penetration testing;

f) knowledge of assessing TSP security controls; and

g) knowledge of product evaluation (e.g. as per ISO/IEC 15408 [i.7]) being able to assess secure operation of evaluated products or trustworthy systems such as cryptographic modules.

6.2.1.8 Audit team

Audit teams shall be competent for the duties assigned to them. The following requirements shall apply to the audit team as a whole. In each of the following areas at least one auditor in the team shall satisfy auditors' criteria for taking responsibility within the audit team:

a) managing the team (lead auditor);

b) demonstrated knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of TSP and information security;

c) demonstrated knowledge of the current technical state-of-art regarding TSP and Public Key Infrastructure;

d) demonstrated knowledge in technologies applicable to the TSP trust service being audited;

e) demonstrated knowledge of performing information security related risk assessments so as to identify assets, threats and the vulnerabilities of the TSP and understanding their impact and their mitigation and control; and

f) demonstrated knowledge of organizational reliability issues.

The audit team should be competent to trace indications of security incidents in the TSP operations back to the appropriate elements of the TSP controls.

An audit team may consist of one person provided that the person meets all criteria set out above.

6.2.1.9 Audit team leader

In addition to the requirements in clause 6.2.1.4, audit team leaders shall have gained the following experiences and skills in audits under guidance and supervision:

a) having acted as auditor in at least three complete TSP audits;

b) having adequate knowledge and attributes to manage the audit process; and

c) having the competence to communicate effectively, both orally and in writing.

7 Process requirements

7.1 General requirements

The requirements from ISO/IEC 17065 [1], clause 7.1 shall apply. In addition, the following TSP-specific requirements and guidance apply.

The evaluation of the TSP and the trust service(s) it provides shall take the form of an audit carried out against defined criteria that should:

a) take into account specificities of the type of trust service to be assessed;

b) ensure that all aspects of the TSP activity are fully covered; and

c) be based on standards, publicly available specifications and/or regulatory requirements.

EXAMPLE: Standards on which those criteria could be based include ETSI EN 319 401 [i.6], ETSI EN 319 411-1 [i.2], or ETSI EN 319 411-2 [i.3] or ETSI EN 319 421 [i.9]. Regulatory requirements on which those criteria could be based include those defined in Regulation (EU) No 910/2014 [i.1].

7.2 Application

The requirements from ISO/IEC 17065 [1], clause 7.2 shall apply.

7.3 Application Review

7.3.0 General requirements

The requirements from ISO/IEC 17065 [1], clause 7.3 shall apply.

For each TSP, the Conformity Assessment Body shall ensure that it does not accept any application for which it is not competent or otherwise unable to carry out audit. The Conformity Assessment Body shall then review the contract with the TSP, based on the results of this competence analysis. In particular, the Conformity Assessment Body shall be able to demonstrate that it is able to:

a) understand the areas of activity of the TSP and the associated business risks;

b) define the competencies needed in the Conformity Assessment Body to certify, in relation to the TSP identified activities, to the concerned trust services it provides, and to the relevant security risks, vulnerabilities and impacts on the TSP; and

c) confirm the availability of the required competences.

7.4 Audit

7.4.0 General requirements

The requirements from ISO/IEC 17065 [1], clause 7.4 shall apply. In addition, the following TSP-specific requirements and guidance apply.

7.4.1 Audit Scope

7.4.1.0 Audit Scope General

The documentation of the Conformity Assessment Body shall include the policies and procedures for implementing the audit process, including check lists used in the audit, and the procedures for assessing the conformity of the TSP and the trust services it provides with the criteria against which the audit is carried out.

The audit team shall audit the TSP and the trust service(s) it provides, covered by the defined scope, against all applicable audit requirements.

The Conformity Assessment Body shall ensure that the scope and boundaries of the trust services of the TSP are clearly defined in terms of the characteristics of the business, the organization, facilities, assets and technology.

The Conformity Assessment Body shall ensure that the TSP's information security risk assessment and risk treatment properly reflect its activities and extend to the boundaries of its trust services activities.

The Conformity Assessment Body shall ensure that interfaces with services or activities that are not completely within the scope of the trust services are included in the TSP's information security risk assessment.

EXAMPLE: Sharing of facilities (e.g. IT systems, databases and telecommunication systems) with other organizations.

7.4.1.1 Audit Team Mandate

The mandate given to the audit team shall be clearly defined and made known to the TSP, and shall require the audit team to examine the structure, policies, procedures, practices, management, and operation of the TSP, and confirm that these meet all the requirements relevant to the scope of certification and that the procedures are implemented and are such as to give confidence in the trust services of the TSP.

When required, the audit team may be complemented by technical experts.

Technical experts cannot be used in place of auditors but advise auditors on matters of technical adequacy in the context of the trust service being subject to audit.

The Conformity Assessment Body shall have a procedure for:

a) selecting auditors and technical experts on the basis of their competence, training, qualifications and experience; and

b) monitoring the performance of auditors during audits.

7.4.1.2 Audit Methodology

The plan for and the date of the audit shall be agreed to with the TSP. The Conformity Assessment Body may adopt reporting procedures that suit its needs but as a minimum these procedures shall ensure that:

a) a meeting takes place, prior to leaving the TSP's premises, between the audit team and the TSP's management to which the audit team provides:

   1) a written or oral indication regarding the conformity of the TSP and the trust service(s) it provides with the criteria against which the audit has been carried out, and

   2) an opportunity for the TSP to ask questions about the findings and their basis.

b) the audit team leader provides the conformity assessment body with a report of its findings as to the conformity of the TSP and the trust service(s) it provides with the criteria against which the audit has been carried out.

The Conformity Assessment Body shall have procedures, which are able to verify if the TSP has established an audit programme or passed other external audits or certifications for the different sites, providing enough evidence that all site relevant requirements, specified in the criteria against which the audit is carried out, are fulfilled.

The Conformity Assessment Body's audit procedures shall not presuppose a particular manner of implementation of a trust service or a particular format for documentation and records.

Audit procedures shall focus on establishing that a TSP and the trust service(s) meet the requirements specified in the criteria against which the audit is carried out.

If network-assisted auditing techniques are intended to be used, the TSP shall be made aware of possible security implications and the audit plan shall identify them, as appropriate.

NOTE: Network assisted auditing techniques can include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the trust service documentation and/or trust service processes.

7.4.2 Audit time

The Conformity Assessment Body shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit and re-assessment audit. The time allocated shall consider the following factors:

a) the size of the trust service scope (e.g. number of information systems used, number of employees, number of certificates issued);

b) complexity of the trust service;

c) the type(s) of business performed within scope of the trust service;

d) extent and diversity of technology utilized in the implementation of the various components of the trust service;

e) number of sites;

f) previously demonstrated performance of the trust service;

g) extent of outsourcing and third party arrangements used within the scope of the trust service;

h) the standards, publicly available specifications and regulatory requirements which apply to the certification; and

i) existing certifications.

EXAMPLE: Existing certifications can include information security management certification according to ISO/IEC 27001 [i.8] or product certification against ISO/IEC 15408 [i.7].

The Conformity Assessment Body shall document the justification of the amount of time used in any initial audit, surveillance audits and re-assessment audit.

7.4.3 Multiple sites

7.4.3.1 When to Consider Sample Based Approach

Where a TSP has a number of sites, the Conformity Assessment Body may consider using a sample-based approach to multiple-site audit where the TSP security management scheme meets the following requirements:

a) Security for all applicable site is administered under control of the TSP's security policy administration; and

b) All applicable sites are subject to the TSP's security management review programme.

Applicable sites for a sample based approach shall be those directly concerned with the operations of the TSP meeting the specified TSP policy requirements.

7.4.3.2 Requirements of Sample Based Approach

When using a sample-based approach, the Conformity Assessment Body shall have procedures in place to ensure the following:

a) the initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined;

b) a representative number of sites have been sampled by the Conformity Assessment Body, taking into account:

   1) the results of internal audits of the central site and the other sites;

   2) the results of management review;

   3) variations in the size of the sites;

   4) variations in the business purpose of the sites;

   5) complexity of the trust service;

   6) complexity of the information systems at the different sites;

7) variations in working practices;

8) variations in activities undertaken;

9) potential interaction with critical information systems or information systems processing sensitive information;

10) whether the site is operated by a sub-contractor or other external organization; and

11) any differing regulatory requirements.

c) the sample should be partly selective based on the above in point b) and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection;

d) every site of the TSP that is subject to significant threats to assets, vulnerabilities or impacts should be included in the sampling programme;

e) the surveillance programme shall be designed in the light of the above requirements and shall, within a reasonable time, cover all sites of the TSP operations unless it can be demonstrated that this does not impact on the results of the audit; and

f) in the case of a nonconformity being observed either at the head office or at a single site, the corrective action procedure shall apply to the head office and to all sites of the TSP operations which may be impacted by the same nonconformity.

The audit shall address the TSP's central site activities to ensure that central security administration is applied to all sites at the operational level. The audit should address all the issues outlined above.

The Conformity Assessment Body shall be prepared to substantiate or justify the number of sites being subject to the audit.

7.4.4 Audit Report

7.4.4.1 Report contents

The audit report provided to the TSP and any other party which has a legal reason for viewing the report shall contain the following information:

a) an account of the audit including a summary of the document review and the standard(s), publicly available specifications and/or regulatory requirements against which the audit is carried out;

b) an account of the audit of the TSP's information security risk analysis;

c) total audit time used and detailed specification of time spent on document review, assessment of risk analysis, on-site audit, and audit reporting; and

d) audit enquiries which have been followed, rationale for their selection, and the methodology employed including sampling methodology and test procedures.

7.4.4.2 Report contents details to be provided

The TSP audit report of findings provided by the audit team leader to the Conformity Assessment Body shall be of sufficient detail to facilitate and support a certification decision and shall contain:

a) areas covered by the audit, including the certification requirements and the sites that were audited, the significant audit trails followed and the audit methodologies utilized;

b) observations made, both positive and negative;

c) details of any nonconformities identified, supported by objective evidence and a reference of these non-conformities to the criteria against which the audit has been carried out; and

d) comments on the conformity of the TSP and the trust services it provides with the criteria against which the audit has been carried out, together with a clear statement of nonconformity, and, where applicable, any useful comparison with the results of previous audits of the TSP and of the concerned trust services.

Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents shall be submitted by the audit team leader to the Conformity Assessment Body as evidence to support the certification decision. Information about the samples evaluated during the audit should be included in the audit report, or in other certification documentation. The report shall consider the adequacy of the internal organization and procedures adopted by the TSP to give confidence in the trust services.

In order to provide a basis for the decision to confirm that the TSP and its trust services being audited meet the defined audit criteria, auditors shall produce clear reports that provide sufficient information to make that decision.

7.4.5 Audit process

7.4.5.1 General preparation for the initial audit

The Conformity Assessment Body shall require that a TSP makes all necessary arrangements for the conduct of the audit, including provision for examining documentation and the access to all areas, including those of sub-contractors, records (including internal audit reports and reports of independent reviews of information security) and personnel for the purposes of audit, re-assessment audit and resolution of complaints.

The Conformity Assessment Body shall require the applicant TSP to provide at least the following information, prior to the onsite audit:

a) general information concerning the trust service and the activities it covers;

b) information about locations, sizes and functions of TSP, and its subcontractor sites, which provide or contribute to provide the trust service;

c) a copy of the documentation on policies and practices that rule the provision and operation of the trust service, and, where required, the associated documentation like IT network infrastructure plans with all relevant systems, manuals and instructions for the operation of the trust service.

7.4.5.2 Audit Process

The objective of the audit is to confirm and certify that the TSP and the trust services it provides complies with the applicable assessment criteria.

Auditors shall review before the audit what records are considered as confidential or sensitive by the TSP such that the audit team could not examine these records during the audit of the TSP. The auditors shall judge whether the records that can be examined demonstrate an effective audit. If auditors conclude that an effective audit is not warranted, the Conformity Assessment Body shall inform the TSP that the audit could take place only when the TSP has accepted appropriate access arrangements to confidential or sensitive information.

This audit shall include visits to the site(s) of the TSP (see also clause 7.4.3 on multi-site sampling).

The Conformity Assessment Body shall agree when and where audit process is conducted with the TSP.

Auditors shall perform their audit of the TSP and its trust services in at least two stages:

- **Stage 1:** This stage focuses on obtain and review the documentation on the TSP and the TSP's audited service(s).
- **Stage 2:** This stage consists in an on-site audit that aims to validate the preliminary audit report findings and to complete the audit of the TSP audited services against the assessment criteria.

7.4.5.3 Stage 1 audit

In preparation for the audit, auditors shall obtain and review the documentation on the TSP and the TSP's audited service(s). Auditors shall make the TSP aware of any further types of information and records that may be additionally required for verification during audit stage 1. In this stage of the audit, the Conformity Assessment Body shall also obtain documentation on the design of the trust service.

The objectives of audit stage 1 are to provide a focus for planning of audit stage 2 by gaining an understanding of the structure and extent of the TSP's audited service(s). Audit stage 1 shall include but shall not be restricted to document review. Other elements that may be included in audit stage 1 are verification of records regarding legal entity, arrangements to cover liability, contractual relationships between TSP and potential contractors operating or providing sub-component services, internal/external audits or certifications, management review, and further investigations with regards to the preliminary audit of the self-declared partial compliances or non compliances.

Auditors shall agree, with the TSP, when and where audit stage 1 is conducted.

Stage 1 reports shall be submitted by the audit team leader to the Conformity Assessment Body. In combination with information held on file, these reports shall at least contain:

a) a description of the organizational structure of the TSP, including the use made and organizational structure of other parties (subcontractors) that provide parts of the trust services being audited;

b) a brief summary of the document review;

c) an account of the audit of the information security risk analysis of the TSP's and its trust services being audited;

d) a brief assessment of the auditor whether stage 2 is likely to succeed and whether additional resources (e.g. technical experts, more auditors) are required for stage 2;

e) audit time spent on document review;

f) any areas of concern on whether the TSP's and its trust services being audited meet the requirements of the applicable audit criteria; and

g) the audit methodology employed for stage 1.

In every case, the document review shall be completed prior to the commencement of audit stage 2.

The results of audit stage 1 shall be documented in a written report including any recommendations regarding planning for conducting the audit stage 2. The stage 1 audit findings, including identification of any areas of concern that could be classified as nonconformity during the stage 2 audit, shall be communicated to the client.

In determining the interval between stage 1 and stage 2 audits, consideration shall be given to the needs of the client to resolve areas of concern identified during the stage 1 audit. The certification body may also need to revise its arrangements for stage 2.

The Conformity Assessment Body shall make the TSP aware of assessment audit stage 2 planning and of the further types of information and records that may be required for detailed verification during audit stage 2.

7.4.5.4 Stage 2 audit

This stage shall always take place at the site(s) of the TSP. On the basis of observations documented of audit stage 1, auditors shall draft an audit plan for the conduct of audit stage 2.

The objectives of audit stage 2 are:

a) to confirm that the TSP adheres to its own policies, objectives and procedures; and

b) to confirm that the implemented trust services conform to the requirements of the applicable audit criteria and abide by the applicable TSP's policies, objectives and procedures.

To do this, the audit shall focus on collecting evidences on the TSP's trust services with respect to:

a) implementation of trust service requirements;

b) trust service related organizational processes and procedures;

c) trust service related technical processes and procedures;

d) implemented information security measures for trust services including IT network protection;

e) trust service related products (trustworthy systems) such as cryptographic modules; and

f) physical security of the relevant TSP sites.

7.4.6 Audit Frequency

There shall be a period of no greater than two years for a full (re-)assessment audit unless otherwise required by the applicable legislation or commercial scheme applying the present document.

NOTE: A surveillance audit can be required by an entitled party at any time or by the conformity assessment body as defined by the surveillance programme according to clause 7.9.

7.5 Review

The requirements from ISO/IEC 17065 [1], clause 7.5 shall apply.

7.6 Certification decision

The requirements from ISO/IEC 17065 [1], clause 7.6 shall apply. In addition, the following TSP-specific requirements and guidance apply.

The certification decision can be of one of the following three natures:

a) certified: the audited trust service fulfils the criteria and is certified conformant.

b) A TSP audit may be passed with pending non-conformities provided that these do not impact the ability of the TSP to meet the the intended service. This certification decision is conditional upon to the implementation of corrective actions within 3 months after conclusion of the audit (depending on the type and criticality of the correction(s)); or

c) not certified: the audited trust service is not certified conformant.

7.7 Certification documentation

The requirements from ISO/IEC 17065 [1], clause 7.7 shall apply. In addition, the following TSP-specific requirements and guidance apply.

The identification of the scope of certification shall include identification of the relevant trust service policy (or policies) and/or trust service(s) where applicable.

The Conformity Assessment Body shall provide the client with formal certification documentation that clearly conveys, or permits identification of the national accreditation body.

7.8 Directory of certified products

The requirements from ISO/IEC 17065 [1], clause 7.8 shall apply. In addition, the following TSP-specific requirements and guidance apply.

The Conformity Assessment Body shall maintain and make publicly accessible up to date information on certified TSPs and certified trust services they provide.

7.9 Surveillance

The requirements from ISO/IEC 17065 [1], clause 7.9 shall apply. In addition, the following TSP-specific requirements and guidance apply.

The Conformity Assessment Body shall define a programme of periodic surveillance and re-assessment that includes on-site audits to verify that TSPs and trust services they provide continue to comply with the requirements. It is recommended that at least one surveillance audit per year is performed in between full (re-)assessment audits.

The following activities shall be part of surveillance audit:

a) review of actions taken on nonconformities identified during the previous audit;

b) review of the multi-site sampling strategy, if sampling was applied in the previous audit;

c) review of any changes in documentation and TSP operation;

d) review of internal audits and management review;

e) treatment of complaints;

f) use of marks and/or any other reference to conformity assessment; and

g) review of any public TSP's statements with respect to its operations (e.g. promotional material, website).

Surveillance audits need not necessarily be full system audits. They shall be planned together with other surveillance activities and shall consider a previously applied multisampling strategy.

In addition, a sample of records relating to the operation of TSP over the historical period since the previous audit shall be examined by the auditor.

Surveillance reports shall contain audit information on clearing of nonconformities revealed previously.

7.10 Changes affecting certification

The requirements from ISO/IEC 17065 [1], clause 7.10 shall apply. In addition, the following TSP-specific requirements and guidance apply.

Changes affecting certification initiated by the client may comprise but are not limited to:

a) major changes in the TSP documentation;

b) changes in TSP policies, objectives or procedures affecting the trust service; or

c) security relevant changes.

EXAMPLE: Changes of trustworthy systems, network security or physical infrastructure measuresnew sites relevant for providing the trust service.

The Conformity Assessment body shall establish a procedure with each client to deal with changes affecting certification. This includes notification of the change and determination of about appropriate conformity assessment activities to assess that ongoing conformity is given. Notification and decision shall be performed before implementation of the measures.

There should be a full re-assessment of the TSP's Trust Services under the following circumstances:

a) whenever there are major changes to the scope;

b) whenever there are major changes to the trust services provided under the scope;

c) whenever a new trust service is included in the scope;

d) when there are major changes of IT systems or business processes used by TSP; or

e) when a major part of the trust services moves to another location.

7.11 Termination, reduction, suspension or withdrawal of certification

The requirements from ISO/IEC 17065 [1], clause 7.11 shall apply.

7.12 Records

The requirements from ISO/IEC 17065 [1], clause 7.12 shall apply.

7.13 Complaints and appeals

The requirements from ISO/IEC 17065 [1], clause 7.13 shall apply.

8 Management system requirements

8.1 Options

The requirements from ISO/IEC 17065 [1], clause 8.1 shall apply.

8.2 General management system documentation

The requirements from ISO/IEC 17065 [1], clause 8.2 shall apply.

8.3 Control of documents

The requirements from ISO/IEC 17065 [1], clause 8.3 shall apply.

8.4 Control of records

The requirements from ISO/IEC 17065 [1], clause 8.4 shall apply.

8.5 Management review

The requirements from ISO/IEC 17065 [1], clause 8.5 shall apply.

8.6 Internal audits

The requirements from ISO/IEC 17065 [1], clause 8.6 shall apply.

8.7 Corrective actions

The requirements from ISO/IEC 17065 [1], clause 8.7 shall apply.

8.8 Preventive actions

The requirements from ISO/IEC 17065 [1], clause 8.8 shall apply.

Annex A (informative): Auditors' code of conduct

Auditors deployed for performing TSP assessment audits should observe a Code of Conduct fulfilling at least the following:

a) To act in a trustworthy and unbiased manner in relation to both the Conformity Assessment Body by which the auditor is employed, contracted or otherwise engaged and any other organization involved in an audit performed by him/her or by personnel directly under his/her control.

b) To act independently and impartially; to disclose to the Conformity Assessment Body deploying him/her any relationships he/she may have or may have had with the organization to be audited and to decline any assignment that could cause or could be perceived as causing conflict of interest.

c) Not to accept any inducement, gift, commission, discount or any other profit from organizations audited, from their representatives, or from any other interested person, nor knowingly allow personnel for whom he/she is responsible to do so.

d) Not to disclose the observations, or any part of them, of the audit team for which he/she is or was responsible or of which he/she is or was part, or any other information obtained in the course of an assessment audit, to any third party unless authorized in writing by both the audited organization and the Conformity Assessment Body by which the auditor is or was deployed.

e) Not to act in any way prejudicial to the reputation or interest of the Conformity Assessment Body by which the auditor is or was deployed.

In the event of any alleged breach of the code of conduct, to co-operate fully in any formal enquiry procedure.

Annex B (informative): Bibliography

- ISO/IEC 19011:2011: "Guidelines for auditing management systems".
- International Accreditation Forum Mandatory Document for the Certification of Multiple Sites Based on Sampling.

History

Document history				
V1.1.1	March 2012	Publication as TS 119 403		
V2.1.1	November 2014	Publication as TS 119 403		
V2.1.1	December 2014	EN Approval Procedure	AP 20150401:	2014-12-02 to 2015-04-01
V2.2.0	June 2015	Vote	V 20150821:	2015-06-22 to 2015-08-21