Draft ETSI EN 319 401 V2.0.0 (2015-06)

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

Reference

REN/ESI-0019401v211

Keywords

electronic signature, provider, 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

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 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):	12 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

Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of security, makes consumers, businesses and administrations hesitate to carry out transactions electronically and to adopt new services. Trust service providers are often an essential element to establish trust between parties transacting electronically, particularly in open public networks, and can be used, for example, to provide trusted identity information and help establish secure communications between transacting parties. Examples of such trust service providers are issuers of public key certificates, time-stamping service providers, providers of remote electronic signature generation or validation services.

For participants of electronic commerce to have confidence in the security of these trust services they need to have confidence that the trust service providers (TSPs) have established a set of procedures, processes and security measures in order to minimize the operational and financial threats and risks associated.

The present document specifies baseline policy requirements on the operation and management practices of TSP regardless the service they provide. Other standards, addressing particular type of trust service, can build on this standard to identify supplement requirements for particular type of trust service.

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.2] and those from CA Browser Forum [i.4].

1 Scope

The present document specifies general policy requirements relating to trust service providers (TSPs) that are independent of the type of TSP whether certificate issuer (qualified or otherwise), timestamp issuer, signature verifier, e-delivery provider or other form of trust service provider. It defines policy requirements on the operation and management practices of TSPs.

Other specifications refine and extend these requirements as applicable to particular forms of TSP. The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE: See ETSI EN 319 403 [i.6]: "Electronic Signatures and Infrastructures (ESI); Requirements for conformity assessment bodies assessing 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 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.

Not applicable.

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] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.2] 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.3] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management".

[i.4] CA/Browser Forum: "Guidelines for the issuance and management of extended validation certificates".

[i.5] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[i.6] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.7] Void.

[i.8] CA/Browser Forum: "Network and certificate system security requirements".

[i.9] Void.

[i.10] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.11] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

[i.12] 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.13] ETSI EN 301 549: "Accessibility requirements suitable for public procurement of ICT products and services in Europe".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [i.11]

relying party: natural or legal person that relies upon an electronic identification or a trust service

NOTE: Relying parties include parties verifying a digital signature using a public key certificate.

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations

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 policy: set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements

NOTE: See clause 6 for further information on TSP policy.

trust service practice statement: statement of the practices that a TSP employs in providing a trust service

NOTE: See clause 6.2 for further information on practice statement.

trust service provider: entity which provides one or more trust services

3.2 Abbreviations

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

CA	Certification Authority
IP	Internet protocol
IT	Information Technology
TSP	Trust Service Provider
UTC	Coordinated Universal Time

4 Overview

Trust services may encompass but should not be limited to the issuance of public key certificates, provision of registration services, time-stamping services, long term preservation services, e-delivery services and/or signature validation services.

These policy requirements are not meant to imply any restrictions on charging for TSP services.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objectives will be met.

NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSP can employ in providing services.

5 Risk Assesment

The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.

The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

NOTE: See ISO/IEC 27005 [i.5] for guidance on information security risk management as part of an information security management system.

The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment options measures chosen as documented in the information security policy and the trust service practice statement (see clause 6).

The risk assessment shall be regularly reviewed and revised.

6 Policies and practices

6.1 Trust Service Practice (TSP) statement

The TSP shall specify the set of policies and practices appropriate for the trust services it is providing. These shall be approved by management, published and communicated to employees and external parties as relevant.

The TSP shall have a statement of the practices and procedures for the trust service provided.

NOTE 1: The present document makes no requirement as to the structure of the trust service practice statement.

In particular:

a) The TSP shall have a statement of the practices and procedures used to address all the requirements identified for the applicable TSP policy.

b) The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP services including the applicable policies and practices.

c) The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the service policy.

d) The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP practice statement.

e) The TSP management shall implement the practices.

f) The TSP shall define a review process for the practices including responsibilities for maintaining the TSP practice statement.

g) The TSP shall notify notice of changes it intends to make in its practice statement and shall, following approval as in (d) above, make the revised TSP practice statement immediately available as required under (c) above.

h) The TSP shall state in its practices the provisions made for termination of service (as per 7..11)

6.2 Terms and Conditions

TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.

These terms and conditions shall at least specify for each trust service policy supported by the TSP the following:

a) the trust service policy being applied;

b) any limitations on the use of the service;

EXAMPLE 1: The expected life-time of public key certificates.

c) the subscriber's obligations, if any;

d) information for parties relying on the trust service;

EXAMPLE 2: How to verify the trust service token, any possible limitations on the validity period associated with the trust service token.

e) the period of time during which TSP event logs are retained;

f) limitations of liability;

g) limitations on the use of the services provided including the limitation for damages arising from the use of services exceeding such limitations;

h) the applicable legal system;

i) procedures for complaints and dispute settlement;

j) whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme; and

k) the TSP contact information.

Customers shall be informed about the limitations in advance.

Terms and conditions shall be made available through a durable means of communication. This information shall be available in a readily understandable language. It may be transmitted electronically.

6.3 Information security policy

The TSP shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.

In particular:

a) A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP facilities, systems and information assets providing the services. The TSP shall publish and communicate this information security policy to all employees who are impacted by it.

NOTE 1: See clause 5.1.1 of ISO/IEC 27002:2013 [i.3] for guidance.

b) The TSP shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSP functionality is undertaken by outsourcers. TSP shall define the outsourcers liability and ensure that outsourcer are bound to implement any controls required by the TSP.

c) The TSP information security policy and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. Any changes that will impact on the level of security provided shall be approved by the TSP high level management body. The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.

NOTE 2: Further specific recommendations are given in the CA Browser Forum network security guide [i.8], item 1.

d) A TSP's management security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP facilities, systems and information assets providing the services.

NOTE 3: See clause 5.1.1 of ISO/IEC 27002:2013 [i.3] for guidance.

7 TSP management and operation

7.1 Internal organization

7.1.1 Organization reliability

The TSP organization shall be reliable.

In particular:

a) Trust service practices under which the TSP operates shall be non-discriminatory.

b) The TSP shall make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP terms and conditions.

c) The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law, to cover liabilities arising from its operations and/or activities.

NOTE: For liability of TSPs operating in EU, see article 13 of the Regulation (EU) No 910/2014 [i.2].

d) The TSP shall have the financial stability and resources required to operate in conformity with this policy.

e) The TSP shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

f) The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

7.1.2 Segregation of duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP assets.

7.2 Human resources

The TSP shall ensure that employees and contractors support the trustworthiness of the TSP's operations.

NOTE 1: See clauses 6.1.1 and 7 of ISO/IEC 27002:2013 [i.3] for guidance.

In particular:

a) The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.

b) TSP personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two. This should include regular (at least every 12 months) updates on new threats and current security practices.