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

EUROPEAN STANDARD

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

Copyright Notification

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.

NOTE 2: Personnel employed by a TSP include individual personnel contractually engaged in performing functions in support of the TSP's services. Personnel who can be involved in monitoring the TSP services need not be TSP personnel.

c) Appropriate disciplinary sanctions shall be applied to personnel violating TSP policies or procedures.

NOTE 3: See clause 7.2.3 of ISO/IEC 27002:2013 [i.3] for guidance.

d) Security roles and responsibilities, as specified in the TSP's management security policy, shall be documented in job descriptions or in documents available to all concerned personnel. Trusted roles, on which the security of the TSP's operation is dependent, shall be clearly identified. Trusted roles shall be named by the management and shall be accepted by the management and the person to fulfil the role.

NOTE 4: See clause 7.2.1 of ISO/IEC 27002:2013 [i.3] for further guidance on management responsibilities in stablishing roles and responsibilities.

e) TSP personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and TSP specific functions. These should include skills and experience requirements.

NOTE 5: See clause 7.2.1 of ISO/IEC 27002:2013 [i.3] for further guidance on management responsibilities in stablishing roles and responsibilities.

f) Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.

NOTE 6: See clause 7.2.1 of ISO/IEC 27002:2013 [i.3] for further guidance on management responsibilities in stablishing roles and responsibilities.

g) Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

h) All TSP personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP operations.

NOTE 7: See clause 6.1.2 of ISO/IEC 27002:2013 [i.3] for guidance.

i) Trusted roles shall include roles that involve the following responsibilities:

  i) Security Officers: Overall responsibility for administering the implementation of the security practices.

  ii) System Administrators: Authorized to install, configure and maintain the TSP trustworthy systems for service management.

  iii) System Operators: Responsible for operating the TSP trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery.

  iv) System Auditors: Authorized to view archives and audit logs of the TSP trustworthy systems.

NOTE 8: Additional application specific roles can be required for particular trust services.

j) TSP personnel shall be formally appointed to trusted roles by senior management responsible for security requiring the principle of "least privilege" when accessing or when configuring access privileges.

k) Personnel shall not have access to the trusted functions until any necessary checks are completed.

NOTE 9: In some countries it is not possible for TSP to obtain information on past convictions without the collaboration of the candidate employee.

7.3 Asset management

7.3.1 General requirements

The TSP shall ensure an appropriate level of protection of its assets including information assets.

NOTE 1: See clause 8 of ISO/IEC 27002:2013 [i.3] for guidance.

In particular, the TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment.

NOTE 2: See clause 8.1.1 of ISO/IEC 27002:2013 [i.3] for guidance.

7.3.2 Media handling

All media shall be handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data shall be securely disposed of when no longer required.

NOTE: See clause 8.3 of ISO/IEC 27002:2013 [i.3] for guidance.

7.4 Access control

The TSP's system access shall be limited to authorized individuals.

In particular:

a) Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties. Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.

b) The TSP shall administer user access of operators, administrators and system auditors. The administration shall include user account management and timely modification or removal of access.

c) Access to information and application system functions shall be restricted in accordance with the access control policy. The TSP system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.

d) TSP personnel shall be identified and authenticated before using critical applications related to the service.

e) TSP personnel shall be accountable for their activities.

EXAMPLE: By retaining event logs.

f) Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

NOTE 1: See clause 9 of ISO/IEC 27002:2013 [i.3] for guidance.

NOTE 2: Further recommendations regarding authentication are given in the CA Browser Forum network security guide [i.8], clause 2.

7.5 Cryptographic controls

Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

7.6 Physical and environmental security

The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security.

NOTE 1: See clause 11 of ISO/IEC 27002:2013 [i.3] for guidance.

In particular:

a) physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals;

NOTE 2: Criticality is identified through risk assessment, or through application security requirements, as requiring a security protection.

b) controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities;

c) controls shall be implemented to avoid compromise or theft of information and information processing facilities; and

d) components that are critical for the secure operation of the trust service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

NOTE 3: See ISO/IEC 27002:2013 [i.3], clause 11.1 for guidance on secure areas.

7.7 Operation security

The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

NOTE 1: See clause 12 of ISO/IEC 27002:2013 [i.3] for guidance.

In particular:

a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into Information Technology's systems.

b) Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software.

NOTE 2: See clause 14 of ISO/IEC 27002:2013 [i.3] for guidance.

c) The integrity of TSP systems and information shall be protected against viruses, malicious and unauthorized software.

d) Media used within the TSP systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.

e) Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

f) Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.

g) The TSP shall specify and apply procedures for ensuring security patches are applied within a reasonable time after they come available. A security patch need not be applied if it would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. The reason for not applying any security patches shall be documented.

NOTE 3: Further specific recommendations are given in the CA Browser Forum network security guide [i.8], item 1 l.

7.8 Network security

The TSP shall protect its network and systems from attack.

In particular:

a) The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services. The TSP shall apply the same security controls to all systems co-located in the same zone.

b) The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP. Not needed connections and services shall be explicitly forbidden or deactivated. The established rule set shall be reviewed on a regular basis.

c) The TSP shall maintain any elements of their critical systems (e.g. Root CA systems see ETSI EN 319 411-1 [i.12]) in a secured zone.

d) A dedicated network for administration of IT systems that is separated from the operational network shall be established. Systems used for administration shall not be used for non-administrative purposes.

e) Test platform and production platform shall be separated from other environments not concerned with live operations (e.g development).

f) Communication between distinct trustworthy systems shall only be established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

g) If external availability of the trust service is required, the external network connection to the internet shall be redundant to ensure availability of the services in case of a single failure. This may be achieved by two different network connections to one of more internet providers.

h) The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

NOTE 1: See item 4c of the CA Browser Forum network security guide [i.8] for guidance regarding the time period.

i) The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant. The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

NOTE 2: See item 4d of the CA Browser Forum network security guide [i.8] for guidance regarding the time period.

7.9 Incident management

System activities concerning access to IT systems, user of IT systems, and service requests shall be monitored.

In particular:

a) Monitoring activities should take account of the sensitivity of any information collected or analysed.

b) Abnormal system activities that indicate a potential security violation, including intrusion into the TSP network, shall be detected and reported as alarms.

NOTE 1: Abnormal network system activities can comprise (external) network scans or packet drops.

c) The TSP IT systems shall monitor the following events:

   i) Start-up and shutdown of the logging functions; and

   ii) Availability and utilization of needed services with the TSP network.

d) The TSP shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.

e) The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

NOTE 2: For TSPs operating within the European Union see Regulation (EU) No 910/2014 [i.2] Article 19.2 and contact the national supervisory body, or other competent authority for further guidance in implementing this article.

f) Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

g) Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.

NOTE 3: See clause 16 of ISO/IEC 27002:2013 [i.3] for guidance.

h) The TSP shall remediate within a reasonable period after the discovery of a critical vulnerability not previously addressed by the TSP. If this is not possible the TSP shall create and implement a plan to mitigate the critical vulnerability or the TSP shall document the factual basis for the TSP's determination that the vulnerability does not require remediation.

NOTE 4: Further recommendations are given in the CA Browser Forum network security guide [i.8] item 4 f).

i) Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

7.10 Collection of evidence

The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

In particular:

a) The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.

b) Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.

c) Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

d) The precise time of significant TSP environmental, key management and clock synchronization events shall be recorded. The time used to record events as required in the audit log shall be synchronised with UTC at least once a day.

e) Records concerning services shall be held for a period of time after the expiration of the validity of the signing keys or any trust service token as appropriate for providing necessary legal evidence and as notified in the TSP disclosure statement.

f) The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

EXAMPLE: This can be achieved, for example, through the use of write-only media, a record of each removable media used and the use of off-site backup.

7.11 Business continuity management

In the event of a disaster, including compromise of the private signing key or trust service credentials, operations shall be restored as soon as possible. In particular, the TSP shall define and maintain a continuity plan to enact in case of a disaster.

NOTE 1: Other disaster situations include failure of critical components of a TSP trustworthy system, including hardware and software.

NOTE 2: See clause 17 of ISO/IEC 27002:2013 [i.3] for guidance.

7.12 TSP termination and termination plans

Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.

In particular:

a) The TSP shall have an up-to-date termination plan.

b) Before the TSP terminates its services at least the following procedures apply:

   i) the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSP. In addition, this information shall be made available to other relying parties;

   ii) TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens;

   iii) the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information; and

   iv) TSP private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved;

   v) where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.

c) The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

d) The TSP shall state in its practices the provisions made for termination of service. This shall include:

   i) notification of affected entities; and

   ii) transferring the TSP obligations to other parties.

e) The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.

7.13 Compliance

The TSP shall ensure that it operates in a legal and trustworthy manner:

In particular:

a) The TSP shall provide evidence on how it meets the applicable legal requirements.

b) Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities. Applicable standards such as ETSI EN 301 549 [i.13] should be taken into account.

c) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

NOTE: TSPs operating in Europe are required to ensure that personal data is processed in accordance with Directive 95/46/EC [i.1]. In this respect, authentication for a service online concerns processing of only those identification data which are adequate, relevant and not excessive to grant access to that service online.

Annex A (informative): Bibliography

- ISO/IEC 27001:2013: "Information technology - Security techniques - Information security management systems - Requirements".

- CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

History

Document history		
V1.1.1	January 2013	Publication
V2.0.0	June 2015	EN Approval Procedure AP 20151016: 2015-06-18 to 2015-10-16