ETSI EN 319 401 V1.1.1 (2013-01)

European Standard

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

Reference

DEN/ESI-000117

Keywords

electronic signature, security

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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:
http://portal.etsi.org/chaircor/ETSI_support.asp

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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

National transposition dates	
Date of adoption of this EN:	8 January 2013
Date of latest announcement of this EN (doa):	30 April 2013
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 October 2013
Date of withdrawal of any conflicting National Standard (dow):	31 October 2013

Introduction

Electronic commerce, in its broadest sense, is emerging as a way of doing business and communicating across public and private networks. An important requirement of electronic commerce is the ability to identify the originator and protect the confidentiality of electronic exchanges. This is commonly achieved by using cryptographic mechanisms and electronic signatures which are supported by Trust Service Providers supporting electronic signatures.

Electronic signatures are used in a large variety of circumstances and applications, resulting in a wide range of services and products related to or using electronic signatures. Such products and services are not limited to the issuance and management of certificates, but also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures.

For participants of electronic commerce to have confidence in the security of these cryptographic mechanisms and/or electronic signatures they need to have confidence that the Trust Service Providers supporting electronic signatures (TSP) have properly established procedures and protective measure in order to minimize the operational and financial threats and risks associated with public key crypto systems, processes and security management.

The present document specifies baseline policy requirements on the operation and management practices of TSP regardless the service they provide.

The present document is derived from the generally applicable requirements specified in TS 101 456 [i.4] "Policy requirements for certification authorities issuing qualified certificates" and TS 102 042 [i.3] "Policy requirements for certification authorities issuing public key certificates".

1 Scope

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

Other policy document specifications refine and extend these requirements as applicable to particular forms of TSP. The present document does not specify how the requirements identified may 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 TS 119 403 [i.8]: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance".

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at 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.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

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] ISO/IEC 27002:2005: "Information technology - Security techniques - Code of practice for information security management".

[i.3] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.4] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.5] Certification Authority (CA)/Browser Forum: "Guidelines for the issuance and management of extended validation certificates".

[i.6] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[i.7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.8] ETSI TS 119 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance".

[i.9] ISO/IEC 27001:2005: "Information technology - Security techniques - Information security management systems - Requirements".

[i.10] ITU-T Recommendation X.509 (11/08): "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".

3 Definitions and abbreviations

3.1 Definitions

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

advanced electronic signature: electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control; and

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. (Directive 1999/93 [i.7]).

attribute: information bound to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity

electronic signature: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data

qualified certificate: certificate which meets the requirements laid down in Annex I of Directive 1999/93/EC [i.7] and is provided by a certification service provider who fulfils the requirements laid down in Annex II of Directive 1999/93/EC [i.7]

qualified electronic signature: advanced electronic signature which is based on a qualified certificate and which is created by a secure signature creation device

NOTE: Under Directive 1999/93 [i.7] article 5.1 Qualified electronic signatures:

a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data; and

b) are admissible as evidence in legal proceedings.

relying party: recipient of a trust service token who acts in reliance on that trust service token

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

secure signature creation device: signature creation device which meets the requirements laid down in Annex III of Directive 1999/93/EC [i.7]

subject: entity identified in a trust service token as the subject entity associated with the private key or other attributes given in the trust service token

subscriber: entity subscribing with a trust service provider

NOTE: A subscriber may be acting on behalf of one or more subjects or other end users or may be a subscriber or end user acting on its own behalf.

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

TSP practice statement: statement of the practices which a TSP employs in issuing, and managing trust service tokens

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 token to a particular community and/or class of application with common security requirements

NOTE: A certificate policy as defined in X.509 [i.10] is an example of a TSP policy. See clause 4.3 for further information on TSP policy and practice statement.

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

NOTE: A certification practice statement as defined in X.509 [i.10] is an example of a TSP practice statement. See clause 4.3 for further information on TSP policy and practice statement.

trust service provider: entity which provides one or more electronic Trust Services

NOTE: This includes Certification-Service-Provider (CSP).

trust service token: physical or binary (logical) object generated or issued as a result of the use of a Trust Service

NOTE: Examples of binary Trust Service Tokens are public key certificates, Certificate Revocation Lists (CRL), Time-Stamp Tokens, Online Certificate Status Protocol (OCSP) responses, evidence of delivery issued by a Registered Electronic Mail (REM) Service Provider.

3.2 Abbreviations

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

TSP	Trust Service Provider

4 General concepts

4.1 Trust Service Provider

Directive 1999/93/EC [i.7] on a Community framework for electronic signatures (hereafter "the Directive ") mainly focuses on Certification Service Providers issuing qualified certificates but it also applies to "*an entity or legal or natural person who issues certificates or provides other services related to electronic signatures*" (Article 2.11). By extending the basic principles of the Directive 1999/93/EC [i.7] this can be applicable to several other types of services ancillary to electronic signatures. These services may encompass but should not be limited to, e.g. the issuance and management of Qualified Certificates as defined in the Directive, the issuance and management of Extended Validation Certificates as defined by the Certification Authority/Browser Forum (CAB Forum) [i.5] provision of registration services, time-stamping services, directory services, validation services, the provision of electronic signature software and hardware including signature-creation devices, and computing services or consultancy services related to electronic signatures. The entity that provides one or more trust electronic service which enhances trust and confidence in electronic transactions is referred in the present document as a Trust Service Provider (TSP).

NOTE: The term Certification Service Provider (CSP) in the Directive refers to a TSP as defined in the present document, providing Trust Services related to electronic signatures.

The TSP may make use of other parties to provide parts of the services. However, the TSP always maintains overall responsibility and ensures that the policy requirements identified in the present document are met. For example, a certification authority may sub-contract all the component services, including the certificate generation service. However, the key used to sign the certificates is identified as belonging to the TSP, and the TSP maintains overall responsibility for meeting the requirements defined in the present document and liability for the issuing of certificates to the public as required in the Directive [i.7].

4.2 Subscriber

The subscriber may be an organization comprising several end-users or an individual end-user.

When the subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

4.3 Trust Service policy and practice statement

This clause explains the relative roles of trust service policy and a trust service practice statement. It places no restriction on the form of a trust service policy or trust service practice statement specification.

4.3.1 Purpose

In general, the purpose of the trust service policy, which may be referenced by a policy identifier in a token, states "what is to be adhered to", while a trust service practice statement states "how it is adhered to", i.e. the processes it will use in providing services. The relationship between the trust service policy and trust service practice statement is similar in nature to the relationship of other business policies which state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.

If any changes are made to a trust service policy which affects the applicability then the policy identifier should be changed.

4.3.2 Level of specificity

A trust service policy is a higher level document than a trust service practice statement; it may apply to a community to which more TSPs belong that abide by the common set of rules specified in that trust service policy. A trust service practice statement defines how one specific TSP meets the technical, organizational and procedural requirements identified in a trust service policy.

NOTE: Even lower-level documents may be appropriate for a TSP detailing the specific procedures necessary to complete the practices identified in the certification practice statement. This lower-level documentation is generally regarded as internal operational procedure documents, which may define specific tasks and responsibilities within an organization. While this lower-level documentation may be used in the daily operation of the TSP and reviewed by those doing a process review, due to its internal nature this level of documentation is considered private and proprietary and therefore beyond the scope of the present document. For example, the policy may require secure management of the private key(s), the practices may describe the dual-control, secure storage practices, while the operational procedures may describe the detailed procedures with locations, access lists and access procedures.

4.3.3 Approach

The approach of a trust service policy is significantly different from a trust service practice statement. A trust service policy is defined independently of the specific details of the specific operating environment of a TSP, whereas a trust service practice statement is tailored to the organizational structure, operating procedures, facilities, and computing environment of a certification authority. A trust service policy may be defined by the users of TSP services, whereas the trust service practice statement is always defined by the provider.

5 Obligations and liability

5.1 TSP obligations

5.1.1 General

The TSP shall ensure that all requirements on TSP, as detailed in clause 6, are implemented as applicable to the service policy.

The TSP has the responsibility for conformance with the procedures prescribed in this policy, even when the TSP functionality is undertaken by sub-contractors.

The TSP shall provide all its services consistent with its TSP practice statement.

5.1.2 TSP obligations towards subscribers

The TSP shall meet its claims as given in its terms and conditions including the availability and accuracy of its service.

5.2 Subscriber obligations

The present document places no specific obligations on the subscriber beyond any TSP specific requirements stated in the TSP's terms and conditions.

5.3 Information for relying parties

The terms and conditions made available to relying parties (see clause 6.2) shall include a notice in order to identify under which conditions is reasonably to rely upon a service.

6 Requirements on TSP practices

The TSP shall implement the controls that meet the following requirements.

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 may employ in providing services.

6.1 Trust Service Practice Statement

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

NOTE 1: This policy 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 in this policy.

b) The TSP's 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.

NOTE 2: The TSP is not generally required to make all the details of its practices public.

d) The TSP shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its services as specified in clause 6.2.

e) The TSP shall have a high level management body with final authority for approving the TSP practice statement.

f) The TSP management shall ensure that the practices are properly implemented.

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

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

6.2 TSP Dissemination of Terms and Conditions

TSP shall ensure that the terms and conditions regarding its services are made available to all subscribers and relying parties.

This statement shall at least specify for each service policy supported by the TSP the following:

a) the trust service policy being applied;

b) the expected life-time of the trust service token and any other limitations on the use of the service;

c) the subscriber's obligations as defined in clause 5.2, if any;

d) information on how to verify the trust service token and any possible limitations on the validity period;

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

f) limitations of liability;

g) the applicable legal system;

h) procedures for complaints and dispute settlement; and

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

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

6.3 Key management life cycle

6.3.1 TSP key generation

The TSP shall ensure, where applicable, that any cryptographic keys are generated under controlled circumstances and are issued securely.

The TSP shall ensure, where applicable, that a cryptography algorithm used for key generation is recognized as appropriate for the time period of the key usage.

6.3.2 TSP key storage, backup and recovery

The TSP shall ensure that TSP private keys remain confidential and maintain their integrity. The TSP shall ensure that TSP private signing keys are not used inappropriately. The TSP shall ensure that TSP private signing keys are not used beyond the end of their life cycle.

6.3.3 TSP public key distribution

The TSP shall ensure that the integrity and authenticity of the TSP signature verification (public) key and any associated parameters are maintained during its distribution to relying parties.

6.3.4 Life cycle management of cryptographic devices used to sign TSP Token

The TSP shall ensure the security of cryptographic device throughout its lifecycle.

6.4 TSP management and operation

6.4.1 Security management

The TSP shall ensure that administrative and management procedures are applied, adequate and correspond to recognized best practice.

NOTE 1: See ISO/IEC 27001 [i.9] and ISO/IEC 27002 [i.2] for guidance on information security management.

In particular:

a) The TSP shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk assessment shall be regularly reviewed and revised if necessary.

NOTE 2: See ISO/IEC 27005 [i.6] for guidance.

b) The TSP shall retain responsibility for all aspects of the provision of services within the scope of its service policy, whether or not functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the TSP and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the TSP. The TSP shall retain responsibility for the disclosure of relevant practices of all parties.

c) The TSP management shall provide direction on information security through a suitable high level steering body that is responsible for defining the TSP's information security policy. The TSP shall ensure publication and communication of this policy to all employees who are impacted by it.

d) The TSP shall have a system or systems for quality and information security management appropriate for the trust services it is providing.

e) The information security infrastructure necessary to manage the security within the TSP shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the TSP management steering body.

f) 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: The TSP's management security policy should identify all relevant targets, objects and potential threats related to the services provided and the safeguards required to avoid or limit the effects of those threats, consistent with the risk assessment. It should describe the rules, directives and procedures regarding how the specified services and the associated security assurance are granted in addition to stating policy on incidents and disasters.

g) TSP shall ensure that the security of information is maintained when the responsibility for TSP functions has been outsourced to another organization or entity.

6.4.2 Asset classification and management

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

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

6.4.3 Personnel security

The TSP shall ensure that personnel and hiring practices enhance and support the trustworthiness of the TSP's operations.

In particular:

a) The TSP shall employ personnel who possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

NOTE 1: TSP personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, 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 may be involved in monitoring the TSP services need not be TSP personnel.

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

c) Security roles and responsibilities, as specified in the TSP's management security policy, shall be documented in job descriptions. Trusted roles, on which the security of the TSP's operation is dependent, shall be clearly identified.

d) TSP personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, 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.

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

f) Managerial personnel shall be employed who possess experience or training in the electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

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

h) Trusted roles include roles that involve the following responsibilities:

- Security Officers: Overall responsibility for administering the implementation of the security practices.
- System Administrators: Authorized to install, configure and maintain the TSP trustworthy systems for service management.
- System Operators: Responsible for operating the TSP trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery.
- System Auditors or evaluators: Authorized to view archives and audit logs of the TSP trustworthy systems.

i) TSP personnel shall be formally appointed to trusted roles by management responsible for security.

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

NOTE 3: In some countries it may not be possible for TSP to obtain information on past convictions without the collaboration of the candidate employee.

6.4.4 Physical and environmental security

The TSP shall ensure that physical access to critical services is controlled and risks related to physical security minimized.

In particular:

a) physical access to facilities concerned with sensitive services shall be limited to properly authorized individuals;

NOTE 1: Sensitive services are those that are 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; and

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

NOTE 2: See ISO/IEC 27002 [i.2] for guidance on physical and environmental security.

6.4.5 Operations management

The TSP shall ensure that the TSP system components are secure and correctly operated, with acceptable risk of failure.

In particular:

a) The integrity of TSP system components and information shall be protected against viruses, malicious and unauthorized software.

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

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

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

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

Media handling and security

f) 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.

Incident reporting and response

g) 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. All incidents shall be reported as soon as possible after the incident.

h) The TSP shall establish procedures to ensure that, without undue delay and where feasible not later than 24 hours after having become aware of it, it notifies the competent supervisory body, the competent national body for information security and other relevant third parties such as providers of software or systems relying on the trust service, data protection authorities 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.

i) Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity.

Operations procedures and responsibilities

j) TSP security operations shall be separated from other operations.

NOTE: TSP security operations' responsibilities include:

- operational procedures and responsibilities;
- secure systems planning and acceptance;
- protection from malicious software;
- backups;
- network management;
- active monitoring of audit journals, event analysis and follow-up;
- media handling and security;
- data and software exchange.

These operations shall be managed by TSP trusted personnel, but, may actually be performed by, non-specialist, operational personnel (under supervision), as defined within the appropriate management security policy, and, roles and responsibility documents.

6.4.6 System access management

The TSP shall ensure that TSP's system access is limited to properly authorized individuals.

In particular:

a) Controls (e.g. firewalls) shall be implemented to protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.

NOTE: Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.

b) Sensitive data shall be protected against unauthorized access or modification. Sensitive data shall be protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure.

c) The TSP shall ensure effective administration of user (this includes operators, administrators and auditors) access to maintain system security, including user account management, auditing and timely modification or removal of access.

d) The TSP shall ensure that access to information and application system functions is restricted in accordance with the access control policy and that the TSP system provides 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 is restricted and tightly controlled.

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

f) TSP personnel shall be accountable for their activities, for example by retaining event logs.

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

6.4.7 Trustworthy systems deployment and maintenance

The TSP shall use trustworthy systems and products that are protected against modification.

NOTE: The risk assessment carried out on the TSP's services should identify its critical services requiring trustworthy systems and the levels of assurance required.

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.

6.4.8 Business continuity management and incident handling

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

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

6.4.9 TSP termination

The TSP shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSP's services, and in particular ensure continued maintenance of information required to verify the correctness of trust service tokens.

In particular:

a) Before the TSP terminates its services the following procedures shall be executed as a minimum:

   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.

   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.

b) 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.

c) 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.

d) 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.

6.4.10 Compliance with legal requirements

The TSP shall ensure compliance with legal requirements.

In particular:

a) The TSP shall ensure it meets all applicable statutory requirements, for protecting records from loss, destruction and falsification.

b) The TSP shall ensure that the requirements of the applicable Privacy and Data Protection regulation (e.g. European Data Protection Directive [i.1]) are met.

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.

d) The information contributed by users to the TSP shall be completely protected from disclosure unless with their agreement or by court order or other legal requirement.

6.4.11 Recording of information concerning operation of the service

The TSP shall ensure that all relevant information concerning the operation of services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings.

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.

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.

NOTE: This may 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.

g) The specific events and data to be logged shall be documented by the TSP.

6.5 Organizational

The TSP shall ensure that its organization is reliable.

In particular that:

a) Policies and procedures 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 has adequate arrangements to cover liabilities arising from its operations and/or activities.

d) It has the financial stability and resources required to operate in conformity with this policy.

e) It has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of the services or any other related matters.

f) It has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

History

Document history			
V1.1.1	March 2012	Public Enquiry	PE 20120705: 2012-03-07 to 2012-07-05
V1.1.1	November 2012	Vote	V 20130108: 2012-11-09 to 2013-01-08
V1.1.1	January 2013	Publication	