**BUREAU OF INDIAN STANDARDS**

*Preliminary Draft*

# इलेक्ट्रॉनिक हस्ताक्षर और इन्फ्रास्ट्रक्चर (ईएसआई) — ट्रस्ट सेवा प्रदाताओं के लिए सामान्य नीति अपेक्षाएँ

# Electronic Signatures and Infrastructures (ESI) — General Policy Requirements for Trust Services Providers

ICS 35.020

Information Technology and Information Technology enabled Services Sectional Committee, SSD 10

FOREWORD

*(Formal clause will be added later)*

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 the present document to identify supplement requirements for particular type of trust service.

The present document is aiming to meet the general requirements to provide trust and confidence in electronic transactions.

**Bureau of Indian Standards**

*Preliminary Draft*
*on*

# ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); GENERAL POLICY REQUIREMENTS FOR TRUST SERVICES PROVIDERS

## 1 SCOPE

The present document specifies general policy requirements relating to trust service providers (TSPs) that are independent of the type of TSP. 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 — Refer ETSI EN 319 403 for details about requirements for conformity assessment bodies assessing Trust Service Providers.

## 2 REFERENCES

The standards listed in Annex A contain provisions, which through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of these standards.

## 3 DEFINITION OF TERMS, SYMBOLS, ABBREVIATIONS AND NOTATION

### 3.1 Term

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

**3.1.1** *Coordinated Universal Time (UTC)* — Time scale based on the second as defined in Recommendation (*source*: ITU-R TF.460-6).

**3.1.2** *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.

**3.1.3** *Subscriber* — Legal or natural person bound by agreement with a trust service provider to any subscriber obligations.

**3.1.4** *Trust Service* — Electronic services for:

a) Creation, verification, and validation of digital signatures and related certificates

b) Creation, verification, and validation of time-stamps and related certificates

c) Registered delivery and related certificates

d) Creation, verification and validation of certificates for website authentication; and

*e)* Preservation of digital signatures or certificates related to those services.

**3.1.5** *Trust Service Component* — One Part of the overall service of a TSP.

*Example:*

Those identified in (*see* **4.4** of ETSI EN 319 411-1). Also, ETSI TS 119 431-1 defines requirements for a Server Signing Application Service Component (SSASC) which can be implemented as part of TSP's service which also includes other service components.

NOTE — Other standards, including ETSI standards, can specify requirements for other service components which can form part of a wider TSP's service.

**3.1.6** *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 — A trust service policy describes what is offered and provides information about the level of the service. It is defined independently of the specific details of the specific operating environment of a TSP; a trust service policy can apply to a community to which several TSPs belong that abide by the common set of rules specified in that policy. It can be defined for example by the TSP, by standards, by national (e.g government) or international organizations, by the customers (subscribers) of the TSP and it is not necessarily part of the TSP's documentation.

**3.1.7** *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.

**3.1.8** *Trust Service Provider (TSP)* — Entity which provides one or more trust services.

**3.1.9** *Trust Service Token* — Physical or binary (logical) object generated or issued as a result of the use of a trust service.

NOTE — Examples of trust service tokens are: certificates, CRLs, time-stamp tokens, OCSP responses.

### 3.2 Symbols

Void.

### 3.3 Abbreviations

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

| Abbreviation | Description |
|---|---|
| CA | Certification Authority |

| | |
|---|---|
| IP | Internet Protocol |
| IT | Information Technology |
| SSASC | Server Signing Application Service Component |
| TSP | Trust Service Provider |
| UTC | Coordinated Universal Time |

### 3.4 Notation

The requirements in the present document are identified as follows:

<the 3 letters REQ> - < the clause number> - <2digit number - incremental>

The management of the requirement identifiers throughout subsequent editions of the present document is as follows:

When a requirement is inserted at the end of a clause, the 2-digit number above is incremented to the next available digit.

When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish a new requirement.

The requirement identifier for deleted requirements are left and completed with "Void"; and

The requirement identifier for modified requirement are left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

## 4 OVERVIEW

Trust services can encompass but is not 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's 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.

When implementing controls of (*see clause* **7**, ISO/IEC 27002:2013) should be applied.

> 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 ASSESSMENT

### 5.1 REQ-5-01

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

### 5.2 REQ-5-02

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 — (source: ISO/IEC 27005:2011 )for guidance on information security risk management as part of an information security management system.

### 5.3 REQ-5-03

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

### 5.4 REQ-5-04

The risk assessment shall be regularly reviewed and revised.

### 5.5 REQ-5-05

The TSP's management shall approve the risk assessment and accept the residual risk identified.

## 6 POLICIES AND PRACTICES

### 6.1 Trust Service Practice statement

**6.1.1** *REQ-6.1-01* — The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.

**6.1.2** *REQ-6.1-02* — The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.

**6.1.3** *REQ-6.1-03A* — The TSP shall have a statement of the practices and procedures used to address all the requirements of the applicable trust service policy as identified by the TSP.

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

**6.1.4** *REQ-6.1-04* — The TSP's trust service practice statement shall identify the obligations of all external *organizations* supporting the TSP's services including the applicable policies and practices.

**6.1.5** *REQ-6.1-05A* — The TSP shall make available to subscribers and relying parties its practice statement, *and* other relevant documentation, as necessary to demonstrate conformance to the trust service policy.

NOTE ― The TSP need not disclose any aspects containing sensitive information in the documentation that is made available to subscribers and relying parties.

**6.1.6** *REQ-6.1-06*— The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP's practice statement.

**6.1.7** *EQ-6.1-07*— The TSP's management shall implement the practices.

**6.1.8** *EQ-6.1-08* — The TSP shall define a review process for the practices including *responsibilities* for maintaining the TSP's practice statement.

**6.1.9** *REQ-6.1-09* — Void.

**6.1.10** *REQ-6.1-09A [CONDITIONAL]* — When the TSP intends to make changes in its practice statement that might *affect* the acceptance of the service by the subject, subscriber or relying parties, it shall give due notice of changes to subscribers and relying parties.

NOTE ─ The due notice does not need to provide the details of the changes. The due notice can be published on the TSP's repository.

**6.1.11** *REQ-6.1-10* — The TSP shall, following approval as in REQ-6.1-06 above, make the revised TSP's practice statement immediately available as required under REQ-6.1-05 above.

**6.1.12** *REQ-6.1-11* — The TSP shall state in its practices the provisions made for termination of service *(see* **7.12***).*

## 6.2 Terms and Conditions

**6.2.1** *REQ-6.2-01* — TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.

**6.2.2** *REQ-6.2-02* — The 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 provided including the limitation for damages arising from the use of services exceeding such limitations;

*Example:*

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*:

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's event logs are retained;

f) limitations of liability;

g) The applicable legal system;

h) Procedures for complaints and dispute settlement;

i) 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;

j) The TSP's contact information; and

k) Any undertaking regarding availability.

**6.2.3** *REQ-6.2-03* — Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

**6.2.4** *REQ-6.2-04* — Terms and conditions shall be made available through a durable means of communication.

**6.2.5** *REQ-6.2-05* — Terms and conditions shall be available in a readily understandable language.

**6.2.6** *REQ-6.2-06* — Terms and conditions may be transmitted electronically.

### 6.3 Information Security Policy

**6.3.1** *REQ-6.3-01* — 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.

**6.3.2** *REQ-6.3-02* — Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

**6.3.3** *REQ-6.3-03* — A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services.

**6.3.4** *REQ-6.3-04* — The TSP shall publish and communicate the information security policy to all employees who are impacted by it.

NOTE — See *clause* **5.1.1** of ISO/IEC 27002:2013 for guidance.

**6.3.5** *REQ-6.3-05* — The TSP shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSP's functionality is undertaken by outsourcers.

**6.3.6** *REQ-6.3-06* — TSP shall define the outsourcers' liability and ensure that outsourcer are bound to implement any controls required by the TSP.

**6.3.7** *REQ-6.3-07* —The TSP's information security policy and inventory of assets for information security *(see* **7.3***)* shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

**6.3.8** *REQ-6.3-08* — Any changes that will impact on the level of security provided shall be approved by the management body referred to in REQ-6.1-07.

**6.3.9** *REQ-6.3-09* — The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.

**6.3.10** *REQ-6.3-10* — The maximum interval between two checks shall be documented in the trust service practice statement.

NOTE — Further specific recommendations are given in the CA/Browser Forum network security guide (*see* item **1**)

## 7 TSP Management and Operation

### 7.1 Internal Organization

**7.1.1** *Organization Reliability*

**7.1.1.1** *REQ-7.1.1-01*— The TSP organization shall be reliable.

**7.1.1.2** *REQ-7.1.1-02* — Trust service practices under which the TSP operates shall be non-discriminatory.

**7.1.1.3** *REQ-7.1.1-03* — The TSP should 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's terms and conditions.

**7.1.1.4** *REQ-7.1.1-04* — The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable 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).

**7.1.1.5** *REQ-7.1.1-05* — The TSP shall have the financial stability and resources required to operate in conformity with this policy.

**7.1.1.6** *REQ-7.1.1-06* — 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.

**7.1.1.7** *REQ-7.1.1-07* — 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.

**7.1.1.8** *REQ-7.1.1-08 [CONDITIONAL]* — When the TSP makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements, it shall maintain overall responsibility for meeting the requirements defined in the trust service policy.

**7.1.1.9** *REQ-7.1.1-09 [CONDITIONAL]* — When the TSP makes use of a trust service component provided by another party it shall ensure that the use of the component interface meets the requirements as specified by the trust service component provider.

**7.1.1.10** *REQ-7.1.1-10 [CONDITIONAL]* — When the TSP makes use of a trust service component provided by another party it shall ensure that the security and functionality required by the trust service component are meeting the appropriate requirements of the applicable policy and practices.

**7.1.2** *Segregation of Duties*

**7.1.2.1** *REQ-7.1.2-01*— Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets.

## 7.2 Human Resources

**7.2.1** *REQ-7.2-01*— The TSP shall ensure that employees and contractors support the trustworthiness of the TSP's operations.

NOTE 1 — see clause **6.1.1** and 7 of ISO/IEC 27002:2013 for guidance.

**7.2.2** *REQ-7.2-02*— 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.

**7.2.3** *REQ-7.2-03* — TSP's 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.

**7.2.4** *REQ-7.2-04* — 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's services need not be TSP's personnel.

**7.2.5** *REQ-7.2-05* — Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures.

NOTE 3 — See *clause* 7.2.3 of ISO/IEC 27002:2013 for guidance.

**7.2.6** *REQ-7.2-06* — Security roles and responsibilities, as specified in the TSP's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel.

**7.2.7** *REQ-7.2-07* — Trusted roles, on which the security of the TSP's operation is dependent, shall be clearly identified.

**7.2.8** *REQ-7.2-08* — Void.

**7.2.9** *REQ-7.2-09* — Void.

NOTE 4 — See clause 7.2.1 of ISO/IEC 27002:2013 for further guidance on management responsibilities in establishing roles and responsibilities.

**7.2.10** *REQ-7.2-10* — TSP's 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* **7.1.2**), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

**7.2.11** *REQ-7.2-11* — Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements.

NOTE 5 — See clause 7.2.1 of ISO/IEC 27002:2013 for further guidance on management responsibilities in establishing roles and responsibilities.

**7.2.12** *REQ-7.2-12* — 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 for further guidance on management responsibilities in establishing roles and responsibilities.

**7.2.13** *REQ-7.2-13* — 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.

**7.2.14** *REQ-7.2-14* — All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations.

NOTE 7 — See clause 6.1.2 of ISO/IEC 27002:2013 for guidance.

**7.2.15** *REQ-7.2-15* — Trusted roles shall include roles that involve the following responsibilities:

a) *Security Officers* — Overall responsibility for administering the implementation of the security practices.

b) *System Administrators* — Authorized to install, configure and maintain the TSP's trustworthy systems for service management.

NOTE 8 — This includes recovery of the system.

c) *System Operators* — Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.

d) *System Auditors* — Authorized to view archives and audit logs of the TSP's trustworthy systems.

NOTE 9 — Additional application specific roles can be required for particular trust services.

**7.2.16** *REQ-7.2-16* — Void.

**7.2.17** *REQ-7.2-16A* — TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security.

**7.2.18** *REQ-7.2-16B* — Trusted roles shall be accepted by the appointed person to fulfil the role.

**7.2.19** *REQ-7.2-17* — Personnel shall not have access to the trusted functions until the necessary checks are completed.

NOTE 10 — 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

**7.3.1.1** *REQ-7.3.1-01* ― 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 for guidance.

**7.3.1.2** *REQ-7.3.1-02* — 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* for guidance.

### 7.3.2 Media Handling

**7.3.2.1** *REQ-7.3.2-01*― 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.

**7.3.2.2** *REQ-7.3.2-02* ― Media used within the TSP's systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.

**7.3.2.3** *REQ-7.3.2-03* ― Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

NOTE — See clause 8.3 of ISO/IEC 27002:2013 for guidance.

## 7.4 Access Control

**7.4.1** *REQ-7.4-01*― The TSP's system access shall be limited to authorized individuals.

**7.4.2** *REQ-7.4-02* — Void.

**7.4.3** *REQ-7.4-03* — Void.

**7.4.4** *REQ-7.4-04* — Void.

**7.4.5** *REQ-7.4-04A* — The TSP shall administer user access of operators, administrators and system auditors applying the principle of "least privileges" when configuring access privileges.

NOTE 1 — This generally applies to personnel appointed to trusted roles as per REQ-7.2-16**.**

**7.4.6** *REQ-7.4-05* — The administration shall include user account management and timely modification or removal of access.

**7.4.7** *REQ-7.4-06* — Access to information and application system functions shall be restricted in accordance with the access control policy.

**7.4.8** *REQ-7.4-07* — The TSP's 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.

**7.4.9** *REQ-7.4-08* — TSP's personnel shall be identified and authenticated before using critical applications related to the service.

**7.4.10** *REQ-7.4-09* — TSP's personnel shall be accountable for their activities.

*Example*:

By retaining event logs.

**7.4.11** *REQ-7.4-10* — Sensitive data shall be protected against being revealed through re-used storage objects (e.g deleted files) or media *(see* **7.3.2***)* being accessible to unauthorized users.

**7.4.12** *REQ-7.4-10* — Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) or media (*see* **7.3.2**) being accessible to unauthorized users.

NOTE 2 — See clause 9 of ISO/IEC 27002:2013 for guidance.

NOTE 3 — Further recommendations regarding authentication are given in the CA/Browser Forum network security guide (*see clause* 2*).*

## 7.5 Cryptographic Controls

**7.5.1** *REQ-7.5-01*— Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

NOTE — See clause 10 of ISO/IEC 27002:2013 for guidance.

## 7.6 physical and environmental security

**7.6.1** *REQ-7.6-01* — 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 for guidance.

**7.6.2** *REQ-7.6-02* — 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.

**7.6.3** *REQ-7.6-03* — Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.

**7.6.4** *REQ-7.6-04* — Controls shall be implemented to avoid compromise or theft of information and information processing facilities.

**7.6.5** *REQ-7.6-05* — 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 clause 11.1 for guidance on secure areas.

## 7.7 Operation Security

**7.7.1** *REQ-7.7-01*— 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 [**Error! Reference source not found.**] for guidance.

NOTE 2 — See *clause 14* of ISO/IEC 27002:2013 [**Error! Reference source not found.**] for guidance on systems acquisition, development and maintenance.

**7.7.2** *REQ-7.7-02* — 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 IT systems.

**7.7.3** *REQ-7.7-03* — Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy.

**7.7.4** *REQ-7.7-04* — The procedures shall include documentation of the changes.

NOTE 4 — See *clause 14* of ISO/IEC 27002:2013 for guidance.

**7.7.5** *REQ-7.7-05* — The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.

**7.7.6** *REQ-7.7-06* — Void.

**7.7.7** *REQ-7.7-07* — Void.

**7.7.8** *REQ-7.7-08* — Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.

**7.7.9** *REQ-7.7-09* — The TSP shall specify and apply procedures for ensuring that:

a) security patches are applied within a reasonable time after they come available;

b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and

c) the reasons for not applying any security patches are documented.

NOTE 5 — Further specific recommendations are given in the CA/Browser Forum network security guide item 1 l.

### 7.8 Network Security

**7.8.1** *REQ-7.8-01*— The TSP shall protect its network and systems from attack.

**7.8.2** *REQ-7.8-02* — 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.

**7.8.3** *REQ-7.8-03* — The TSP shall apply the same security controls to all systems co-located in the same zone.

**7.8.4** *REQ-7.8-04* — The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP.

**7.8.5** *REQ-7.8-05* — The TSP shall explicitly forbid or deactivate not needed connections and services.

**7.8.6** *REQ-7.8-06* — The TSP shall review the established rule set on a regular basis.

**7.8.7** *REQ-7.8-07*— The TSP shall keep all systems that are critical to the TSP's operation in one or more secured zone(s) (e.g Root CA systems *see* ETSI EN 319 411-1).

**7.8.8** *REQ-7.8-08* — The TSP shall separate dedicated network for administration of IT systems and TSP's operational network.

**7.8.9** REQ-7.8-09 — The TSP shall not use systems used for administration of the security policy implementation for other purposes.

**7.8.10** REQ-7.8-10 — The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g development, test and staging systems).

**7.8.11** REQ-7.8-11 — Void.

**7.8.12** *REQ-7.8-11A* — The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

**7.8.13** *REQ-7.8-12* — If a high level of availability of external access to the trust service is required, the external network connection shall be redundant to ensure availability of the services in case of a single failure.

**7.8.14** REQ-7.8-13 — 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.

**7.8.15** *REQ-7.8-13A* — The vulnerability scan requested by REQ-7.8-13 should be performed once per quarter.

**7.8.16** *REQ-7.8-14* — 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.

**7.8.17** *REQ-7.8-14A* — The penetration test requested by REQ-7.8-14 should be performed at least once per year.

**7.8.18** *REQ-7.8-15* — 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.

**7.8.19** *REQ-7.8-16* — Controls (e.g firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.

**7.8.20** *REQ-7.8-17* — Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.

### 7.9 Incident Management

**7.9.1** *REQ-7.9-01* ― System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored.

NOTE 1 — See *clause 16 of ISO/IEC 27002:2013* for guidance.

**7.9.2** *REQ-7.9-02* — Monitoring activities should take account of the sensitivity of any information collected or analysed.

**7.9.3** *REQ-7.9-03* — Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms.

NOTE 2 — Abnormal network system activities can comprise (external) network scans or packet drops.

**7.9.4** *REQ-7.9-04* — The TSP shall monitor the following events:

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

b) Availability and utilization of needed services with the TSP's network.

**7.9.5** *REQ-7.9-05* — 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.

**7.9.6** *REQ-7.9-06* — 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.

**7.9.7** *REQ-7.9-07* — 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 within 24 hours of the breach being identified.

**7.9.8** *REQ-7.9-08* — 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.

**7.9.9** *REQ-7.9-09* — The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.

**7.9.10** *REQ-7.9-10* — The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.

**7.9.11** *REQ-7.9-11*— For any vulnerability, given the potential impact, the TSP shall [CHOICE]:

a) create and implement a plan to mitigate the vulnerability; or

b) 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 item 4 f).

**7.9.12** *REQ-7.9-12*— 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

**7.10.1** *REQ-7.10-01* — 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.

NOTE — See requirement REQ-7.13-05.

**7.10.2** *REQ-7.10-02* — The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.

**7.10.3** *REQ-7.10-03* — Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.

**7.10.4** *REQ-7.10-04* — 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.

**7.10.5** *REQ-7.10-05* — The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.

**7.10.6** *REQ-7.10-06* — The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.

**7.10.7** *REQ-7.10-07* — Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions *(see* **6.3***)*.

**7.10.8** *REQ-7.10-08* — 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 or by parallel storage of the information at several (e.g 2 or 3) independent sites.

### 7.11 Business Continuity Management

**7.11.1** *REQ-7.11-01* **—** The TSP shall define and maintain a continuity plan to enact in case of a disaster.

**7.11.2** *REQ-7.11-02* **—** In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g a security vulnerability) with appropriate remediation measures.

NOTE 1 — See *clause 17 of ISO/IEC 27002:2013* for guidance in the event of a disaster.

NOTE 2 — Other disaster situations include failure of critical components of a TSP's trustworthy system, including hardware and software.

### 7.12 Tsp Termination and Termination Plans

**7.12.1** *REQ-7.12-01* **—** 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.

**7.12.2** *REQ-7.12-02* — The TSP shall have an up-to-date termination plan.

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

**7.12.3** *REQ-7.12-03* — Before the TSP terminates its services, 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, TSPs and relevant authorities such as supervisory bodies.

**7.12.4** *REQ-7.12-04* — Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties.

**7.12.5** *REQ-7.12-05* — Before the TSP terminates its services, the 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.

**7.12.6** *REQ-7.12-06* — Before the TSP terminates its services, 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.

**7.12.7** *REQ-7.12-07* — Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

**7.12.8** *REQ-7.12-08* — Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.

**7.12.9** *REQ-7.12-09* — 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.

**7.12.10** *REQ-7.12-10* — The TSP shall state in its practices the provisions made for termination of service. This shall include:

a) notification of affected entities; and

b) where applicable, transferring the TSP's obligations to other parties.

**7.12.11** *REQ-7.12-11*— 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

**7.13.1** *REQ-7.13-01* **—** The TSP shall ensure that it operates in a legal and trustworthy manner.

**7.13.2** *REQ-7.13-02* — The TSP shall provide evidence on how it meets the applicable legal requirements.

**7.13.3** *REQ-7.13-03* — Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.

**7.13.4** *REQ-7.13-04* — Applicable standards on accessibility such as ETSI EN 301 549 should be taken into account.

**7.13.5** *REQ-7.13-05* — 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 1 — TSPs operating in India are required to ensure that personal data is processed in accordance with the DPDP Act, 2023 as and when it is effective

NOTE 2 — See ISO/IEC 27701:2019 for requirements and guidance on the extension to 27002 for privacy information management.

## Annex A

*(Clause* 2)

## INFORMATIVE REFERENCES

| *IS No./Other Publications* | *Title* |
|---|---|
| ISO/IEC 27002:2013 | Information technology - Security techniques - Code of practice for information security management |
| CA/Browser Forum | Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates |
| ISO/IEC 27005:2011 | Information technology - Security techniques - Information security risk management |
| ETSI EN 319 403 | Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers |
| CA/Browser Forum | Network and certificate system security requirements |
| Recommendation ITU-R TF.460-6 (2002) | Standard-frequency and time-signal emissions |
| ETSI EN 319 411-1 | Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements |
| ETSI EN 301 549 | Accessibility requirements for ICT products and services |
| ETSI EN 319 411-2 | Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates |
| (EU) 2016/679 | Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC |
| ETSI TS 119 431-1 | Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev |
| ISO/IEC 27701:2019 | Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines |