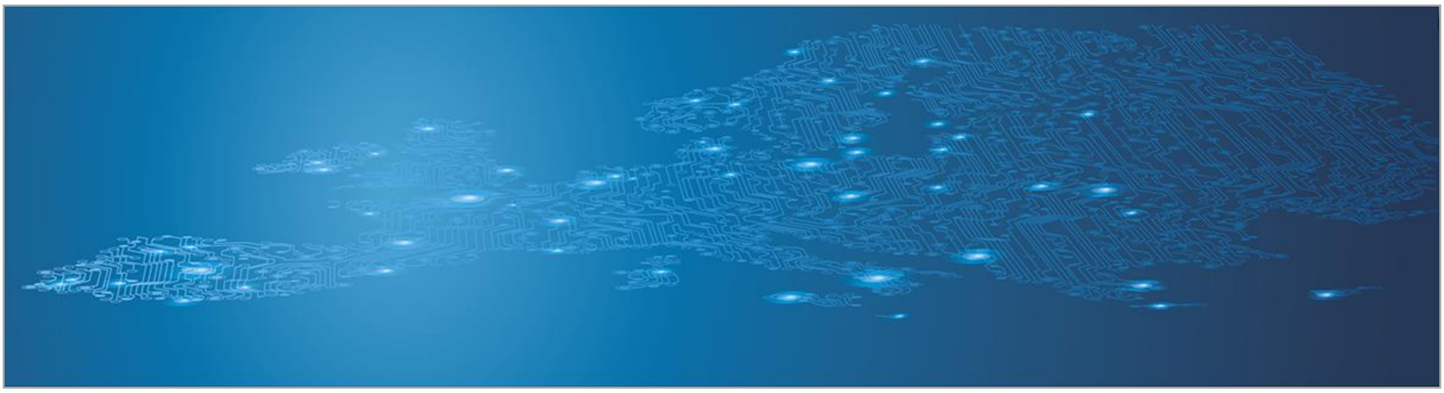

Auditing Framework for TSPs

Guidelines for Trust Service Providers

Version 1.0 – December 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Iñigo Barreira, Izenpe

Arno Fiedler, Nimbus Technologieberatung GmbH

Artur Miękina, Polish Security Printing Works

Clemens Wanko, TUV Informationstechnik GmbH

Sławomir Górniak, ENISA

Contact

For contacting the authors please use sta@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank the numerous experts from governmental entities, industry, foundations and trust service providers who reviewed this paper for their contributions.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-121-2

Executive summary

In order to remove barriers for cross-border trust services and having regard to results from successful European projects like STORK, which have shown that technical issues of interoperability can be overcome, the European Parliament and the Council of the European Union adopted on 27 July 2014 the Regulation on electronic identification and trusted services for electronic transactions in the internal market[1] that replaced the Directive 1999/93/EC on a community framework for electronic signatures, which provided for the legal recognition of electronic signatures. The Regulation strengthens the provisions for interoperability and mutual recognition of electronic identification schemes across borders, enhances current rules for electronic signatures and provides a legal framework for other types of trust services (electronic seals, electronic delivery services, electronic documents, time stamping services and web site authentication).

Trust Services – as the name suggests – require a trustful provision of the corresponding service. The word trustful has to be defined in this context as highly reliable for the user, that the service promised is being delivered strictly according to:

- Terms and conditions of the Trust Service Provider,
- Standards (like ETSI/CEN/ISO),
- Legal requirements as well as according to
- State of technology (like cryptographic algorithms and parameter sets).

In order to support Trust Service Providers (TSPs) in providing information on how audits typically are carrie dout , ENISA has compiled this auditing framework for TSP services.

This report provides an overview of the dedicated means of auditing for TSPs.It discusses specifically the following areas:

- Obligations, warranties and liability of TSPs
- Standards applicable to TSPs and Conformity Assessment Bodies (auditors)
- Methodology of auditing TSPs (off- and on-site)
- TSPs documentation (plans, policies and procedures)
- Implementation of TSPs services

This set of good practices can be used as reference for both, Trust Service Providers (preparing for audits), and Conformity Assessment Bodies (performing audits), in the field of external audits (internal assessments are part of company's risk management procedures, therefore this topic is not covered here). It focuses on measures that can be taken at organizational level, drawing to norms and standards for technical details.

These guidelines are applicable to the same juridic constituency as the eIDAS Regulation. With the entry of the Regulation into service, national differences in legal or regulatory systems will be abolished.

Examples given in this paper consist relate mainly to trust service providers issuing certificates, however, they apply also to other trust service providers and to all trust services, as defined in the Regulation.

[1] 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, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

Table of Contents

1 Introduction

Trust Services – as the name suggests – require a trustful provision of the corresponding service. The word trustful has to be defined in this context as highly reliable, that the service promised is being delivered strictly according to:

- Terms and conditions of the Trust Service Provider,
- Standards (like ETSI/CEN/ISO) as they apply on each class of product or service,
- Legal requirements in place in the jurisdiction of the issuing authority and/or the reporisotry and or the subscriber and/or of the relying party, as well as according to
- State of the art in technology area at hand (like cryptographic algorithms and parameter sets, public key encryption etc.).

In order to show that a trust service provider (TSP) is in line with these points, it could just issue a self-declaration stating that the afore-mentioned requirements are met. It is up to the subscriber as well as up to the parties using or relying upon those trust services to rate the level of trust they like to put on such a self-declaration. The TSP might strictly follow any requirements as claimed in its declaration – or it might not.

In order to overcome the eventuality of lack of conformance with declarations, a cross verification through an independent third party is an adequate solution. This independent party usually compares by means of one or more audits whether the complete operations of a TSP follows the necessary requirements. The results are stated in a conformity assessment (audit) report usually combined with a statement of compliance.

Nowadays a TSP can confirm its compliance with certain national or international standards by providing a corresponding conformity assessment (audit) report of an accredited independent body. This is in many cases a prerequisite before the TSP is allowed to start its business in that area.

In order to support TSPs information on how audits typically are being performed, ENISA has compiled this auditing framework for TSP.

This document provides an overview of the dedicated means of auditing for TSP.

1.1 Why audit

There is typically one of three or a combination of three different reasons for a TSP to require a statement of compliance and herewith the necessary audits:

1. Legal requirements, like the eIDAS[2] regulation,
2. Marketing or
3. Customer requirements.

In case of conformance to legal requirements, the TSP typically has to prove compliance to a supervisory body (SB) in order to be allowed to start up and offer its trusted services. In case of marketing, the TSP expects a sales advantage for its services if he can show its reliability; in terms of customer requirements a TSP customer requires an independent statement of compliance before buying the trust services.

[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, further called ‘eIDAS Regulation’.

1.2 General concept

The diagram below provides an overview of dependencies between various players in the TSP assessment scheme under the eIDAS Regulation (or in general for audits checking compliance to supervisory bodies). For other types the 'Supervisory body' should be replaced by an appropriate entity.

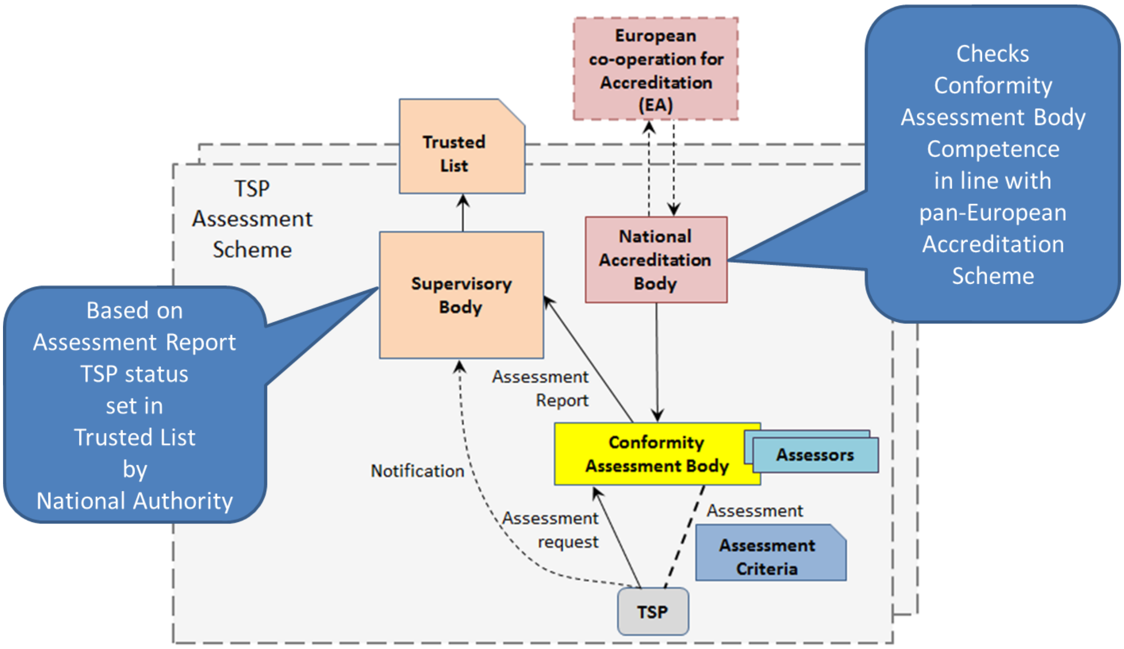
European co-operation for Accreditation (EA)
Checks Conformity Assessment Body Competence in line with pan-European Accreditation Scheme
Trusted List
TSP Assessment Scheme
Supervisory Body
National Accreditation Body
Based on Assessment Report TSP status set in Trusted List by National Authority
Assessment Report
Conformity Assessment Body
Assessors
Notification
Assessment request
Assessment
Assessment Criteria
TSP

Figure 1: TSP Assessment Scheme

1.3 Liability of TSPs

Governing Law, especially Regulation 910/2014 on eIDAS , indicates that all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under that Regulation, specifically with the article 19 (Security requirements applicable to trust service providers). Every national legislation on electronic signatures and on personal data protection should provide a procedure serving to demonstrate that the TSP is applying the current national regulations, which are not affected by the transnational ones, such as the new regulation.

The intention or negligence of a qualified trust service provider should be presumed unless it proves that the damage occurred without the presumed intention or negligence on its part.

The eIDAS Regulation states:

(37) This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles,

this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.

2 Standards applicable to TSPs and Conformity Assessment Bodies

2.1 Regulation

The new EU Regulation on eIDAS and the local law as defined by the different EU member states have to be considered and followed by a TSP.

2.2 Standards related to TSPs

In order to demonstrate good practice according to the state of the art requirements, a TSP might want to claim conformance to one (or more) of the documents listed in the following section below.

Current Standards on policy requirements (ETSI)

Reference	Short Title	Replaces
EN 319 411-2	Policy requirements for certification authorities issuing qualified certificates	TS 101 456
EN 319 411-3	Policy requirements for Certification Authorities issuing public key certificates Note: Excludes web site certificates based on CAB Forum requirements.	TS 102 042
TS 102 042	Policy requirements for Certification Authorities issuing public key certificates Note: Includes requirements for web site certificates based on CAB Forum requirements. For other Non-qualified certificates use EN 319 411-3	
TS 102 023	Policy requirements for time-stamping authorities	
TS 102 158	Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates	

Current Standards on certificate profiles (ETSI)

Reference	Short Title	Replaces
TS 119 412-2	Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons	TS 102 280
EN 319 412-5	Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile	TS 101 862

Upcoming Standards on policy requirements (ETSI)

Reference	Short Title	Replaces
EN 319 411-1	Common policy requirements for certification authorities Note: Incorporates requirements for web site certificates with requirements previously specified in 319 411-3	TS 102 042 EV & Baseline policies EN 319 411-3

EN 319 411-2 (Update)	Policy requirements for certification authorities issuing qualified certificates Note: Extends requirements in part 1 with specific requirements for qualified certificates	EN 319 411-2
EN 319 421	Policy Requirements for Trust Service Providers providing Time-Stamping Services	TS 102 023

Upcoming Standards on certificate profiles (ETSI)

Reference	Short Title	Replaces
EN 310 412-1	Profiles for Trust Service Providers issuing certificates; Part 1: Overview and common data structures	
EN 319 412-2	Part 2: Certificate profile for certificates issued to natural persons	TS 119 412-2 & TS 102 280
EN 319 412-3	Part 3: Certificate profile for certificates issued to legal persons	
EN 319 412-4	Part 4: Certificate profile for web site certificates issued to organizations	
EN 319 412-5	Part 5: Qualified certificate statements for qualified certificate profiles	EN 319 412-5 v1.1.1 & TS 101 862
EN 319 422	Time stamping profile	TS 101 861

Other standards to take into consideration (IETF, ISO)

Reference	Short Title	Replaces
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and CRL profile	
RFC 6960	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP	
RFC 3161	Internet X.509 Public Key Infrastructure Time Stamp Protocol – TSP	
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	
ISO 31000	Family of standards relating to risk management	

2.3 Standards related to Conformity Assessment Bodies

Current Standards (ETSI)

Reference	Short Title	Replaces
TS 119 403	Trust Service Provider Conformity Assessment - General requirements and guidance	
SR 003 091	Recommendations on Governance and Audit Regime for CAB Forum Extended Validation and Baseline Certificates	
TR 101 564	Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs	
TR 103 123	Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates	
TS 103 090	Conformity Assessment for Trust Service Providers issuing Extended Validation Certificates	

Upcoming standards (ETSI)

Reference	Short Title	Replaces
EN 319 403	Trust Service Provider Conformity Assessment	TS 119 403

3 Methodology

This section will describe the typical audit methodology applied by conformity assessment bodies, split into three parts. It also provides distinction between obligations of the TSP and the conformity assessment body.

3.1 Audit procedures

Each of PKI infrastructures shall be assessed regularly according to eIDAS requirements. Compliance should be made by qualified and independent personnel

The audit or assessment procedure shall include the assessment of the documentation as well as the assessment of the implementation. It shall be finalized with the conformity assessment report providing all results and other relevant details of the assessment.

During the Stage 1 (document) assessment phase typically the following documentation is checked:

- Security policy (CP/CPS)
- Documentaion and forms used by TSP processes
- Risk management related documentation
- Business continuity related documentation
- Incident management related documentation
- Terms and conditions
- Contractual documents with third parties
- Insurance and business continuity related documents
- Internal audit plan as well as results (see section 4.1.8)
- Evidences for secure and conformant operations like logs and protocols
- …

During the on site assessment phase (audit) evidences, records and logs of every action should be kept safe and recorded to be handed over to the CAB.

The stage 2 assessment (on site audit) typically addresses the following aspects:

- Compliance with the relevant TSP related standards
- Compliance with TSP operating procedures and principles
- Management of the infrastructure
- Asserting agreed service levels
- Inspection of audit trails, logs, relevant documents etc.

3.1.1 Stage 1 assessment - off site (documentation)

At this stage a TSP will:

- Provide a set of documentation to the conformity assessment body for the first step of the assessment.

The conformity assessment body will check documentation against:

- Requirements of claimed standards,
- Use of appropriate crypto measures (algorithm and parameter sets, cryptographic devices),
- Use of other appropriate security measures.

Background

At Stage 1 the conformity assessment body checks compliance of the TSP on the level of its documentation.

Documentation needs to be drafted at a suitable level of detail[3] in order to understand the security measures taken by the TSP and in order to judge the effectiveness of those measures. It has to describe any relevant TSP services implemented as well as the procedures the TSP uses in order to establish its services (see section 6 for an overview of the services). Doing this, the TSP should reference and explain the mechanisms used in order to gain evidences on its proper operations (any logging and reporting, supervision internal auditing, risk analysing, etc.).

Documentation needs to be up to date, indicating all major/critical changes performed since last assessment, and must reflect the current organization and operation of the TSP.

Only when the stage 1 is completed, the conformity assessment body can proceed to the stage 2. In principle all issues arising at Stage 1 should be resolved, however minor remaining open issues can be treated during stage 2. Precondition for this is however that general issues are solved before the stage 2 can begin.

3.1.2 Stage 2 assessment - on site (implementation)

At this stage a TSP will:

- Provide additional and/or latest sets of documentation (if changed after Stage 1 accomplishment)
- Provide evidence of proper operations
- Provide results of tests performed on its own
- Implement and support tests required by the conformity assessment body
- Demonstrate its operations on an organizational level

The conformity assessment body will:

- Check the latest documentation provided
- Check the results of the TSP tests provided
- Perform technical tests supported by the TSP
- Verify organizational operations

Background

At Stage 2 the conformity assessment body compares the document based description as provided by the TSP in stage 1 against their practical operations. Goal of the stage 2 assessment is for the TSP to demonstrate compliance of its operations for all relevant TSP processes (refer to section 7 for an overview) with the claimed standard and common state of the art security measures. The TSP will therefore take the conformity assessment body through its technical and organizational processes. In order to underline the TSPs conformant operation across the past time period (usually period since last assessment), a convincing set of evidence documentation should be shown to the auditor. Evidence documentation typically contains amongst others:

- Staff training protocols
- Staff trustworthiness evidence
- Role lists including role history

[3] Please refer to the Section 5 for detailed information.

- Access control (physical and IT) lists including history
- Access control logs and reports
- Incident response and follow-up
- Development and update of risk management
- IT security logs and follow-up (protocol server, integrity checker, IDS, etc.)
- Internal audits results

In case testing is required in order to demonstrate compliance, the TSP may already have test results of its own tests or of third party ones that can be rendered available to the auditor. Depending on the standard claimed by the TSP, the conformity assessment body might be allowed to reuse the test results of the TSP. Where provision of own test results by the TSP is not possible or appropriate, additional tests may be required. In such cases, and for reasons of test economics, the TSP needs to prepare and perform the tests under supervision of the conformity assessment body.

In case of minor deviations from the claimed standard during stage 2 assessment, the TSP can take the opportunity for corrective actions. The conformity assessment body may then be able to immediately judge the updated processes.

After a successful stage 1 and stage 2 assessment the conformity assessment body will suggest certification to the certification body.

3.2 TSP conformity assessment report

Upon receipt of a positive assessment report, the supervisory body will perform a quality check of the assessment performed and documented by the conformity assessment body. Only if the assessment had a positive result and it has been carried out according to the rules and requirements of the standard claimed by the TSP, the supervisory body will accepts the result for further treatment like a possible listing on the Trusted List..

The validity scheme of certificates issued by the certification body are coherent with the standards claimed by the TSP. Example: Certificates according to ETSI standards can be issued with a validity of up to three years, while eIDAS Regulation puts an obligation of auditing qualified TSPs every two years (no obligation for non-qualified TSPs).

The TSP needs to order surveillance and re-assessments with a suitably accredited conformity assessment body according to the requirements of the standards claimed. In order to stay certified the TSP must show conformance during surveillance and re-assessments respectively. Example: The certification cycle for a certification according to eIDAS is two years. During the initial assessment typically the complete TSP operations will be audited. During surveillance audits usually only changed processes and evidences of proper operations are audited as well as spot checks of the TSP operations are performed.

Surveillance audits can only be performed as long as the essential TSP procedures stay unchanged.

A template of conformity assessment report can be found in a separate document accompanying this report.

4 TSPs documentation

The increase of corporate governance requirements have caused companies to examine their internal control structures, including documentation, more closely to ensure that controls are in place and operating effectively.

The TSPs should draft security policies and plans taking into account business input and ensuring that roles and responsibilities are defined and implemented, threats and vulnerabilities are identified, security infrastructures and control frameworks (standards, procedures, etc.) are implemented and periodic reviews and test are conducted.

Plans and policies ensure cohesion between expectations and TSPs goals and objectives.

Procedures, standards, evidences are different components that support the implementation of the TSP organizational and also security policy.

Plans and policies communicate TSP´s expectations which are fulfilled though the execution of procedures and adherence to standards and guidelines and that can be demonstrated with the evidences recorded.

This documentation should be written and communicated at a level that is understood by every member of the TSP.

The TSPs should have an internal document list in which specifies all the plans and policies, the procedures to implement those and evidences recorded.

TSPs documentation is one of the essential components and defines an agreed set of rules for the operation and management of the TSP.

These rules cover usage from the various points of views depending of the defined role:

- Users
- Relying Parties
- Service providers

This section describes most of the rules which are used to build and maintain PKI infrastructure. Operation of the PKI within these rules helps to form a cohesive trust platform authentication, encryption and digital signing purposes.

4.1 Plans

Plans are high-level statements of the objectives of the organization. For the purpose of lack of misunderstandings, it’s advisable that these documents::

- Cover all policy areas (explained later in this section)
- Be accurate and comprehensive
- Use direct wording
- Avoid technical implementation details
- Be precise
- Provide navigation to the different procedures that apply
- Be periodically reviewed by management and adjusted.

There are different types of policies and plans but all should include the organizational plan or policy, the functional aspects or issue-specific ones, the system specific and the different levels they apply.

For a TSP, the following documents are needed:

4.1.1 Systems management plan

Systems evolve continuously and in the era we live today they get obsolete very quickly with software and hardware providers offering updates and new solutions.

There should be a plan to manage the entire TSP infrastructure during all the time they operate and to collect appropriate system logs, paying special attention to:

- Status of the servers based on the evolving of the generic software and hardware
    - CPU status: consume, load, use, etc.
    - Storage status
    - Memory status: main, paging in-out, etc.
    - Number of processes running
    - Load balancing
- Status of the infrastructure, adapting the solutions to the new implementations based on standards
- Status of the DB: table spaces, data files, file systems
- Status of the networking devices,
- Status of security controls (firewalls, IPSs)
- Supervision and surveillance

4.1.2 Organization structure

Organizations exist as a system of coordinated activities to accomplish organization objectives. Formalized, written policies, standards, procedures and guidelines are created to provide stability to the organization regardless of the incumbent occupying the position.

The TSP structure is managed in a hierarchical manner, with the lower levels of the TSP having more defined, repetitive tasks and in the higher levels with greater capability to accomplish higher priority tasks.

The plan shall indicate the roles and responsibilities of all the personnel of the TSP, including separation of duties to avoid employees with role conflicting issues and granting least privilege method. It should also propose enforcement measures and methods of maintaining discipline.

4.1.3 Security plan

The TSP should have a security plan, based on existing standards. It shold be consistent with other plans, described further:

- Communication plan
- Risk Management Plan
- Business Continuity Plan
- Incident management plan
- Audit plan
- Training plan
- Legal enforcement plan
- Access control plan

On top of this, it should also include:

- Operations requirements
- Physical and logical security controls
- Personnel control
- Technical controls

4.1.4 Communication plan

The TSP should have a communication plan to spread out all the information internally within the organization and externally for all potential customers and users. This plan may indicate different communication methods for different services, different audience, etc.

The plan should distinguish what type of information is published and how, the target audience and the possible implications that information can produce on the TSP. It should have a different procedure for the internal communication to the employees and the external one to announce a new product for example.

Various categories of communications require specific provisions:

- Internal communication (to the management and to employees)
- Emergency communication (in case of failure/danger/breach)
- Business communication (to customers)
- Media communication
- Shareholders communication

4.1.5 Risk Management Plan

As the networked world continues to shape and impact every aspect of our lives, threats to the global industry continue in parallel.

Security management is the glue that ensures the risks are identified and an adequate control environment is established to mitigate those risks.

There is a need to manage the risks by defining and controlling threats and vulnerabilities. To achieve this, it is important to understand the principles behind the management of risk and the concepts underlying the risk management process.

In order to conduct a risk assessment, several methodologies exist. Please refer to ENISA Guidelines for trust service providers – part 2: Risk assessment[4] and other ENISA work[5].

4.1.6 Business Continuity Plan

This document should address the preparation and processes to ensure the preservation of the TSP business in the face of major disruptions to normal business operations. This involves the identification, selection, implementation, testing and updating of the processes and procedures to protect business from the effects of a major system and network disruptions and to ensure the timely restoration of business operations.

For this BCP, two additional plans should be implemented, a contingency plan and a disaster recovery plan.

4.1.6.1 Contingency plan

A contingency plan can have several phases, each of one has to be described and checked, and these phases can be:

Detection

The TSP should be able to detect a possible incident in order to prevent future incidents based on systems or services degradation and to facilitate information to analyse, solve and learn from these

[4] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp2-risk

[5] http://www.enisa.europa.eu/activities/risk-management

incidents. The TSP should be proactive more than reactive to avoid a possible incident. To perform these proactive tasks all TSP systems and services should be monitored. Besides, for the detection of incidents, there´s a need for operation support 24x7 and also a helpdesk where different users can notify possible incidents or services malfunctions.

The plan should indicate an approximate time to detect any type of incidents.

Notification

The TSP shall have the option that anyone can notify a possible incident that has been detected. The TSP should be able to distinguish from a real incident and a false alarm. Severe incidents should be notified to the responsible team.

The plan should indicate an approximate time to notify and incident

Validation

The validation is the process in which a notified incident is real and has been validated by those roles of the TSP responsible for that.

Evaluation

The TSP should be able to indicate and evaluate the type of the incident, cataloguing them into high, medium and low level and assigning them this criticism should be also corresponded with an appropriate response time.

Activation

The activation phase includes the mechanisms to solve the incident after being catalogued.

Resolution and follow-up

The TSP should indicate what has been done to fix the issue or solve the incident and a follow up of the incident to decide if deactivate the contingency plan

Recording

The TSP shall document the causes of the incident and what effects has produced the effectiveness of the measures taken (response time and time to recover the service or system, etc.) and what improvements can be taken.

An example of a contingency measure can be a backup plan. This plan should indicate what type of backup is going to be performed, at what intervals, when, etc. It should indicate what media is going to be used, for what reason, and where to be stored. This means that it can be in-site backups, which are going to be kept in the same location of the main systems, and off-site backups which are on other locations but controlled.

This plan should define the methods, scope, periodicity, systems involved and indicate in the procedure the tools and technical instructions to perform the backup and also the recovery process.

The plan should also indicate the recovery procedures, type and testing.

4.1.6.2 Disaster recovery plan (DRP)

The DRP strategies should be developed to address the resources requirements. It should define and agree upon functional and technical requirements for recovery strategies. Analysis and availability of critical recovery resources is important to develop ongoing recovery cost estimates. There should be strategies for IT and for business processes. For example, in the IT area, there some requirements for consideration, including:

- Systems hardware resources
- Systems data storage requirements
- Unique (i.e., nonstandard) hardware resources
- Distributed systems (workstations, extranet, intranet, etc.

This plan should be maintained, tested and should also be subject of training.

4.1.7 Incident management plan

The TSP should have a plan to manage all the incidents that affect the normal operation of the TSP. This plan should be aligned with the Business Continuation Plan and Disaster Recovery Plan and include the type of the incident: failure or malfunction, threat, vulnerability or a breach, and how to react, including, the detection, identification, communication, treatment and ending.

4.1.8 Audit plan

This document should cover the general auditing plan and compliance to the claimed standards and law. It reflects policy in the TSP indicating what assessments are going to be performed on what standards and legal documents (as an example, data protection law).

This plan should require a program or schedule on the different assessment including those external and internal. The external ones are referred to those performed by external assessors with the goal of getting the certification in any of the standards related to the TSP´s businesses (e.g. ETSI EN 319 411-2) meanwhile the internal ones are performed by the TSP itself, or subcontracting an external company, to follow and meet the requirements and thus also to show the external assessors of the compliance.

The assessments, both internally and externally, should include at least the most crucial elements of the TSP (CAs and the RAs in case of certificate issuers) and the network security requirements.

Besides, some additional assessments related to those could be:

- Integrity assessment including files, logs, users, providers, etc.
- Documentation revision assessment
- Physical and logical security controls assessment
- Systems and its maintenance assessment
- Application developments assessment

While draftingthis policy,some important steps have to be taking into consideration, among them:

- Understanding legal and business issues concerning auditing
- Analyse critical processes in TSP environment
- Build good TSP processes e.g. (security mechanisms, organization, change management, etc.)
- Create/use evaluation criteria for TSP processes

4.1.9 Training plan

Given today´s complex TSP business environments, the TSP should educate its members regarding most of the aspects concerning the TSP businesses.

Training provides guidance surrounding the TSP functions in general, for example in IT, like security, risk management, etc. and educated users aid the organization in the fulfilment of its program objectives, which may also include audit objectives for organizations that are bound by regulatory compliance.

There are many topics that should be covered by training, such as:

- Corporate security policies
- Regulatory compliance requirements for the organizations
- Business continuity and disaster recovery
- Cryptography, algorithms, PKI
- Risk assessments
- Standards compliance
- Physical and logical infrastructure

The training plan should inform employees about their roles and responsibilities and expectations surrounding their roles.

4.1.10 Legal enforcement plan

The TSPs should have a plan to address the legal acts, regulations, compliance and standards that affect the TSP. It should address the major legal systems nationally and internationally, all regulations affecting the services provided by the TSP and standards and compliance to follow up.

The TSPs shall follow at least the following laws:

- EU Regulation 910/2014 on eIDAS
- National laws related to electronic signatures
- Personal data protection laws

Other laws to consider:

- Contract laws
- Insurance laws
- Industry specific provisions; etc.

4.1.11 Access control plan

Controlling access to systems, services, resources and data is critical to any TSP.

The TSP should produce an access control policy to clearly identify, authenticate, authorize and monitor who or what is accessing the assets of the TSP in order to protect the company from threats and vulnerabilities.

This plan should have a collection of mechanisms that work together to protect the assets of the TSP by aligning people, process and technology allowing them to reduce exposures, build efficiencies, and have confidence in their control environment.

Access controls essentially encompass:

- Facilities
- Support systems
- Information systems
- Personnel

These controls should check and specify:

- Which users can access the system
- What resources they can access
- What operations they can perform

4.2 Policies

Policies are sets of rules intended to influence and determine the way of proceeding in specific caes and areas.

4.2.1 Certification Policy

The RFC 3647 defines a Certification Policy (CP) as *a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements*.

In general, as mentioned above, there are two major categories of Certification Policies:

- Focused on indication applicability of a certificate to a particular community (e.g. Geographical region, specific market – finance, assurance etc.)
- Focused on indication applicability of a certificate to class of application with common security requirements (e.g. different level of security and level of assurance)

Certification Policy is represented in a certificate by a unique number called an “Object Identifier" (OID) which can be registered and is assigned to a particular organization.

Certification Policy also constitutes a basis for an audit, accreditation, or another assessment of a TSP.

4.2.2 Archiving Policy

The archiving policy is an internal document maintained by the TSP staffs, which describes:

- TSP critical information which should be archived due to business continuity and legal requirements

Additionally can be found archive aspects like:

- Influence legal and compliance requirements in archiving issues;
- Consideration which TSP information should be archived;
- Establish what aspects of the TSP system need to be considered for archiving. (e.g. logs, digitally signed data, keys and certificates)
- Decisions (another documents) after implementation archiving policy

4.2.3 Internal Policy Approval Body

Internal Policy Approval Body is a body established to control and maintain the creation and update of Certificate Policies, review Certification Practice Statements, review the results of the TSP audits for policy compliance. The main document describing the organization and responsibilities of that body is accepted by the Management Board (or other designated body) of an organization where PKI infrastructure is established.

4.3 Procedures

The procedures are step-by-step instructions in support of the plans and policies. They indicate how plans or policies will be implemented and define roles and responsibilities.. A Procedures provide clarity and a common understanding of the operations required to support plans or policies on a consistent and regular basis.

At best, the procedures should be developed with the input of each of the interfacing areas. This reduces the risk that important steps, communication, or required deliverables are left out. Consistent documentation of the procedures permits the ability to improve.

4.3.1 Operations security

Operations security is about protection and control of the information assets in the TSP environment. The aim of this procedure is to secure all the operations performed by the TSP. It encompasses a set of tasks to ensure the availability of all TSP resources.

This procedure may be divided into different areas:

- Roles and responsibilities for trusted personnel Operators
  - System administrators
  - Security administrators
  - Auditors
- Different resources protection
  - Facilities/assets
  - Hardware
  - Software
  - Documentation
- Continuity of operations
  - BCP and DRP
- Change control management

4.3.2 Change control management procedure

TSP systems experience frequent changes. Software packages are added, removed or modified. New hardware is introduced.

The rapid advancement of technology requires a proper change management control procedure to maintain the necessary integrity of the system. This procedure is embodied in policies, procedures and operational practices.

The TSP should indicate the scope of the affecting systems (i.e. only production) and should cover all kind of modifications, permanent changes, temporary changes and emergency changes, with a particular procedure for all of them.

These should be defined accordingly and should be a responsible of every asset to be modified. This procedure may have a workflow indicating at least:

- Identify the change: documentation and affected services and products
- Technical evaluation and risks associated: check the viability of the change. Documentation
- Approval of the change by the responsible if previous tests passed
- Information of the change according to the communication policy
- Execution of the change. Documentation of the steps done
- New testing to validate the change.

A detailed inventory of hardware and software is necessary for a recovery and integrity purposes.

4.3.3 Risk analysis procedure

For information on the risk analysis procedure, please consult ENISA guidelines published in 2013[6].

[6] https://www.enisa.europa.eu/activities/identity-and-trust/trust-services/guidelines-tsp

4.3.4 Network security procedure

Networking security includes the structures, transport methods and formats and all security measures used to provide integrity, availability, authentication and confidentiality for transmissions over private and public networks.

Network security is one of the main keys for a TSP because loss of network connectivity, internally or/and externally, may have devastating consequences

The procedure for controlling the security of the network should consist on a list of actions to be taken at different levels, such as:

- General protection, physical and logical of the network on any level
  - Segmentation network on different zones, defining a high-level one for specific requirements
  - Configuration of all networking devices (firewall, switches, routers, etc.)
  - Application of security patches
  - Grant specific permissions to appropriate trusted personnel
- Trusted roles and system accounts
  - Definition of roles and responsibilities for the trusted personnel
  - Procedures on authentication and access control
- Logs, monitoring and alerts
  - Procedure to monitor all the networking infrastructure, configuring alerts and recording logs for assessments
  - Implementation of procedure for detection and prevention on networking vulnerabilities

4.3.5 Incident response procedure

The incident response procedure should define all the processes to follow during the report and management of the incident according to the plan. These processes might indicate how to response depending on the type of the incident, indicating what level of importance and response time should have, whom and how to communicate the incident and a procedure with all the tasks

4.4 Evidence management

Evidence is collected with a view to provide information and demonstrate the effectiveness of the procedures. Measurement of this information provides the ability to improve the processes of the procedures

Evidences collected may be grouped in several sections

4.4.1 Documentation of evidences

The TSP should obtain, for every policy or procedure defined, evidence that all these documents are followed up and consistently what the content of the documentation.

It can be aided with different tools to manage all this type of information. For example, there are tools for performing risk analysis and control and management of all assets, where they are located, used for and by, relations with other assets, characteristics and functionalities, etc.

4.4.2 Test management

The TSP should record all the tests done in their infrastructure, for example, the BCP and DRP once a year, the issuance, validation and revocation processes, etc.

4.4.3 Agreements and contracts

All the contracts, NDAs, SLAs, confidentiality agreements, etc. signed with third parties, employees, customers or users should be maintained and kept safe for preventing the company in case of disputes.

4.4.4 Evaluation reports and testing

The TSP should control all the backup processes having evidences that the backups have been performed correctly and make recovery tests, partially (i.e. a file or a table space) or totally.

Audits should record observations, minor and major non conformities to be fixed.

Personnel should have been trained and record the evidence

All systems, hardware, software and applications should undergo evaluation report on a regular basis to control the effectiveness and functionality and record the evidences

4.4.5 Event logs

All actions performed by the TSP produce logs that should be recorded

4.4.6 Legal compliance records

The TSP shall record all evidences of their legal compliance related to data protection law, national regulations, etc.

4.5 Certification Practice Statement (CPS)

Certification Practice Statement (CPS) is the document supporting the Certification Policies (see 5.2) describing the operating part of public key certification process, participants of this process (Certification Authorities, Registration Authorities, Subscribers and Relying Parties) and describing the areas of application of certificates obtained as its result. CPS should answer for question "how…"

Structure of the Certification Practice Statement documents is mostly based on one of the documents below:

- RFC 3647 "Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework"
- EN 319 411-3 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates"

This document is focused on ETSI EN 319 411-3 and it can be easy to compare with RFC 3647[7] which is more detailed

The structure mentioned above can be divided on 9 components (chapters):

1. Introduction
2. Publication and Repository Responsibilities
3. Identification and Authentication
4. Certificate Life-Cycle Operational Requirements
5. Facilities, Management, and Operational Controls
6. Technical Security Controls
7. Certificate, CRL, and OCSP Profile

[7] http://www.ietf.org/rfc/rfc3647.txt

8. Compliance audit and other assessments
9. Other Business and Legal Matters

A Certification Practice statement is a lower level document than the Certification Policy. The approach of a Certificate Policy is different from a Certification Practice Statement because Certification Policy is defined independently of the specific details of the specific operating environment of a TSP whereas a Certification Practice Statement is tailored to the organizational structure, operating procedures, facilities, and computing environment of a TSP (see 5.2)

A Certificate Policy may be defined by the users of certification services, whereas the Certification Practice Statement is always defined by the TSP.

4.5.1 Introduction

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the Certification Practice Statement document is targeted. It can be found a short overview of Certification Practice Statement, it's identification by name and OID (object identifier).

Additionally there is a short description about certificate usage (for what purposes CA will be issuing certificates), PKI participants and their responsibilities (Certification Authorities, Registration Authorities, Subscribers, Relying Parties – please consult the Definitions section of this report) and Certification Practice Statement administration (contact, organization, approval). Introduction chapter is also a place for Definitions and Acronyms which are used in whole Certification Practice Statement.

4.5.2 Publication and Repository Responsibilities

In this short chapter it can be found all necessary information about CA services which are usually available in online publicly accessible repository. Repository contains any applicable provisions regarding:

- Identification of the entity or entities that operate repositories within the PKI, such as a CA
- Responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status of such certificates
- Frequency of publication
- Access control on published information objects including Certification Policies, Certification Practice Statements, certificates, certificate status, and CRLs

In practice, in repository these are direct URL addresses to CA webpage.

4.5.3 Identification and Authentication

This component describes the procedures used to verify the identity of the natural person (Subscriber) or legal person (Organization) prior to certificate issuance. Each of them must prove possession of the companion private key for the public key being registered, for example, a digital signature in the certificate request message. In this component it could be found identification and authentication requirements for organizational identity of Subscriber, individual Subscriber or person acting on behalf of an organizational Subscriber, or the Organization itself.

It also describes how parties requesting re-key or revocation are authenticated.

In case of rekey it can be distinguished two options:

- First option is for routine re-key such as a re-key request that contains the new key and is signed using the current valid key and:
- Second option for re-key after certificate revocation. In that situation it is necessary to start the process of initial identity validation once again

In the case of revocation there should be special procedures for revocation request

This component also consists of elements regarding naming and identification of the Subscribers:

- Types of names assigned to the subject, such as distinguished names
- Whether names have to be meaningful or not
- Whether or not subscribers can be anonymous or pseudonymous, and if they can, what names are assigned to or can be used by anonymous subscribers
- Rules for interpreting various name forms
- Whether names have to be unique
- Recognition, authentication, and the role of trademarks

4.5.4 Certificate Life-Cycle Operational Requirements

This component is used to specify requirements for whole certificate life-cycle beginning from certificate application ending with loss of the validity of the certificate.

The first step is certificate application where are described details concerning submitting a certificate application by the Subscriber and responsibilities in connection with this process (for example signing agreement). The typical flow relies on generating the key pair and sends a certificate request to the RA. The RA validates and signs the request and sends it to the CA. A CA or RA may have the responsibility of establishing an enrolment process in order to receive certificate applications. In the meantime the issuing CA and RA may perform identification and authentication procedures to validate the certificate application. After that, the CA or RA will either approve or reject the certificate application and after approval the process of issuing certificate is started. Issuing of the certificate should be accepted by Subscriber (either CA or RA) – content of the certificate should be checked carefully before the first usage of keys and certificates.

Subscriber should be also aware of responsibilities relating to the use of keys and certificates, for example that usage of the private key and certificate should only be made in appropriate and dedicated applications according to key usage field. Use of a private key and certificate are subject to the terms of the Subscriber agreement, the use of a private key is permitted only after the subscriber has accepted the corresponding certificate.

A certificate has its own validity period. Before the expiring of this period, the subscriber can renew the existing certificate to establish new validity period.

The subscriber can also apply for certificate re-key meaning that the new key pair should be generated and a new certificate be issued. If there are changes in the certificate content, it can be modified.

The subscriber can check the status of the certificate using the Certificate Revocation List (CRL) or the Online Certificate Status Protocol (OCSP).

4.5.5 Facility, Management, and Operational Controls

This component describes non-technical security controls in all areas concerning CA, RA, Subscribers and others participants. These are physical, procedural, and personnel controls which describe key generation process, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

This part of PKI environment is critical for the whole technical infrastructure because each operation in PKI should be made in correct way described in this component and other internal documents.

Building PKI it is necessary to keep in mind all important requirements from non-technical point of view like:

- Site location and construction (special zones, locked rooms, safe boxes, etc.)
- Physical access with access control mechanism between areas, monitoring of security zones, etc.
- Power and air conditioning
- Water exposures
- Fire prevention and protection
- Media storage (separate location)
- Waste disposal
- Off-site backup

After preparing a suitable place for PKI, the next step is to manage the trusted roles. They should be described together with the responsibilities and tasks for each role. Separation of duties for each role is also essential

In typical PKI it can be distinguished the following roles:

- Security officer
- System Auditor
- System Administrator
- System Operator

For each of roles it should be hired a suitable staff with expected qualifications and experience but also with clear criminal records, references. All staff should be trained and equipped in necessary knowledge and have the awareness of sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on personnel, for example.

To maintain a secure PKI environment it is necessary to implement audit procedures to describe event logging and audit systems, which include for example:

- Types of events recorded
- Frequency with which audit logs are processed or archived
- Period for which audit logs are kept
- Protection of audit logs
- Others

All audit records should be archived and protected against modification, deletion and unauthorized access to the data.

Each TSP should also be ready for special procedures including:

- CA re-key procedures including providing a new CA public key to Subscribers;
- Disaster recovery plan in case of CA compromise or another disaster;
- Procedure for a CA or RA termination

4.5.6 Technical Security Controls

This chapter is an area of technical controls where can be found several important things concerning:

- Key pair generation and installation (key size, cryptographic algorithms, key usage, etc.)

- Private key protection and technical securities of cryptographic modules (private key activation and destruction method, private key escrow, backup and archival etc.);
- Other aspects of key management (public key archival, certificate operational periods,)
- Data Activation (PINS, passwords, or manually-held key shares)
- Computer security controls (e.g. identification and authentication, trusted path)
- Life cycle technical controls:
  - Network security controls (maintaining a high-level network security including firewalls, communication encrypted, antivirus protection, intrusion detection etc.)
- Time-stamping – additional service for marking various data with trusted time (timestamp token)

4.5.7 Other Business and Legal Matters

This chapter covers general business and legal matters.

In first of them there is a possibility to find out about fees to be charged for various services and the financial responsibility of all participants (Subscribers and Relying parties)

The remaining part of information concerned with legal matters (e.g. confidentiality of business information, privacy of personal information, intellectual property rights, warranties, liability, indemnities, others).

4.6 Profiles

Profiles shall be indicated and described either in the practice statement or in the specific policy

4.6.1 Certificate profile

In accordance with IETF PKIX RFC 5280 the Certificate profile shall include:

- Version number(s) supported
- Certificate extensions populated and their criticality
- Cryptographic algorithm object identifiers
- Name forms used for the CA, RA, and subscriber names
- Name constraints used and the name forms used in the name constraints
- Applicable Certification Policy Object Identifier(s)
- Usage of the policy constraints extension
- Policy qualifiers syntax and semantics; and
- Processing semantics for the critical Certification Policy extension

4.6.2 CRL profile

In accordance with IETF PKIX RFC 5280 the CRL profile shall include:

- Version numbers supported for CRLs; and
- CRL and CRL entry extensions populated and their criticality

4.6.3 OCSP profile

In accordance with IETF PKIX RFC 6960 the OCSP shall include:

- Version of OCSP that is being used as the basis for establishing an OCSP system; and
- OCSP extensions populated and their criticality

4.6.4 Others

There are other services e.g. Time Stamp Protocol (TSP) in accordance with IETF PKIX RFC 3161.

5 Implementation

This subdivision of services is only for the purposes of clarification and places no restrictions on any subdivision of an implementation of the TSP services.

5.1 Registration Service

This service is often provisioned by the Registration Authorities (RAs), which have formal (legal) agreement with a Certification Authority (CA)

Registration Authorities identify applicants, subscribers and holders of certificate keys, verify the documentation accrediting the circumstances appearing in the certificates, and validate and approve requests to issue, revoke and renew certificates.

The RAs should assume the following obligations:

- To validate the identity and other personal details of the applicant, subscriber and key owner in the certificates or information relevant for the purpose of the certificates in accordance with these procedures
- To keep all of the information and documentation concerning certificates, and manage their issuance, renewal, revocation or reactivation
- To notify the CA for certificate revocation requests with due diligence and in a fast and reliable manner
- To allow the CA access to its procedures archives and audit logs in order to perform its functions and maintain the necessary information
- To inform the CA of all issuance, renewal, reactivation requests and any other aspects related to the certificates issued
- To validate, with due diligence, the circumstances for revocation that might affect certificate validity
- To comply with the procedures established by the TSP and with the current legislation in this area, in its management operations connected with the issuance, renewal and revocation of certificates
- Where applicable, it can perform the function of making available to the key owner the technical procedures for signature creation data (private key) and electronic signature verification (public key)

It is TSP's responsibility to carry out the subscriber's identification properly. This process should be carried out prior to issuing the certificate.

If the information is not correct, the RA will deny the request and contact the applicant to explain why. If it is correct, the certificate will be issued.

The acceptance of a certificate constitutes the subscriber's acceptance of the terms and conditions of the contract which determines the rights and obligations of the TSP and the subscriber's understanding of the provisions of this CPS, which governs the technical and operational aspects of the digital certification services provided by the TSP.

5.2 Certificate Generation Service

Subscriber certificates can be issued either by means of a cryptographic device or a software mechanism.

1. Issuance procedure for certificates issued using a cryptographic device:

- The Registration Authority authenticates the validity of the documentation submitted by the applicant
- Following authentication, the Registration Authority requests a certificate from the CA
- After verifying that the request has come from an authorized Registration Authority, the CA issues the certificate according to the established procedures and sends it to the Registration Authority
- After the Registration Authority has ascertained that the request comes from the CA, it then downloads the certificate to the signature creation device using a secure cryptographic device management process

2. Issuance procedure for certificates issued using a software mechanism:
   - The Registration Authority authenticates the validity of the documentation submitted by the applicant
   - Together with the application form, the applicant generates a key pair in the server itself giving the public key
   - After receiving the documentation and the public key, the CA issues the certificate
   - The private key and the certificate are created and stored on the cryptographic device or the computer of the subscriber.

5.3 Subject device provision service

This service prepares, and provides or makes available a signature-creation device to subjects for the case stated in section 6.2 when using a cryptographic device

5.4 Dissemination service

This service disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the TSP's terms and conditions, and any published policy and practice information, to subscribers and relying parties.

Method for private key delivery to the different entities:

- Certificates issued on a cryptographic hardware device: private keys for authentication and electronic signature are delivered on a cryptographic device. According to the ETSI TS 419241, the keys can be also delivered remotely.
- Certificates issued on a software mechanism: the private key is generated by the server. It does not need to be delivered

5.5 Revocation service

This service processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.

There are different reasons to revoke subscriber certificates or CA certificates.

5.5.1 Reasons for revoking a subscriber certificate

The TSP shall provide a process for Subscribers to request revocation of their own certificates. The process shall be described in the Certificate Policy or Certification Practice Statement. The qualified TSP shall maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

- A revocation request is made by the signer, the natural or legal person represented by the signer, an authorized third party, or a natural person who applied for a digital certificate for a legal person

    - If revocation is requested by someone other than the signer, subscriber or key owner, the TSP should inform the certificate key owner and subscriber of the revocation of its certificate and specifying the reason for revocation
- The signature creation data of the signer or the certification service provider has been compromised or if the signer or a third party has misused the data
- When a legal or administrative order has been issued to this effect
- Termination of the signer's legal person, death of the signer, termination of the legal person represented by the signer, total or partial unforeseeable incapacity of the signer or person represented by the signer, termination of the representation, dissolution of the legal person represented, change in the circumstances of the safekeeping or use of the signature creation data included in the certificates issued to a legal person
- The TSP terminates its activity, except in cases where the signer has given his or her consent for electronic certificate management services to be transferred to another certification service provider
- Change in the data supplied in order to obtain the certificate or modification in the circumstances verified for certificate issuance
- The certificate is lost, stolen or rendered useless due to damage to the certificate media, or when the support has been changed to another support not envisaged in the certification policy
- One of the parties breaches its obligations
- An error is detected in the certificate issuance procedure, either because one of the prerequisites has not been satisfied or due to technical problems during the certificate issuance process
- There is a potential threat to the security of the systems and the reliability of certificates issued by the TSP for reasons other than the compromise of signature creation data.
- Technical failure in the issuance and/or distribution of certificates or associated documentation

Once the revocation has been duly processed by the RA, the revocation will be made immediately effective in accordance with current legislation.

The TSP shall provide third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates through a readily accessible online means.

5.5.2 Reasons for Revoking a Subordinate CA Certificate

The TSP shall revoke a Subordinate CA certificate if one or more of the following occurs:

- The Subordinate CA requests revocation in writing
- The Subordinate CA notifies that the original certificate request was not authorized and does not retroactively grant authorization
- Obtains evidence that the Subordinate CA’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise
- Obtains evidence that the Certificate was misused
- Is made aware that the Certificate was not issued in accordance with the applicable Certificate Policy or Certification Practice Statement
- Determines that any of the information appearing in the Certificate is inaccurate or misleading
- The Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate
- Revocation is required by the Certificate Policy and/or Certification Practice Statement

5.6 Validation service

This service provides certificate status information to relying parties. This may be based upon revocation lists or an online service which provides status information on an individual basis.

There are mainly two different methods to validate or check the current status of a certificate, which are Certificate Revocation Lists (CRL) and the use of the Online Certificate Status protocol (OCSP)

The TSP should immediately publish the status of a certificate if its status has changed, however some TSPs declare in their policies the maximum time for reaction.

5.6.1 CRL

The CRL contains the stipulated time for issuance of a new CRL, although a CRL may be issued prior to the time indicated on the previous CRL. If there are no revocations, the Certificate Revocation List may be regenerated on a daily basis.

There are some recommendations that a CRL for end entity certificates should be issued at least every 24 hours or when a revocation occurs, and should be valid for 10 days.

The CRL for the CA certificates (ARLs) should be issued every 12 months or when a revocation occurs.

Use of the CRL access service will require:

- In all cases, checking the latest CRL issued that can be downloaded at the URL address contained in the certificate extension “CRL Distribution Point”
- The user also checking the CRL(s) relevant to the hierarchy certificate chain
- The user making sure that the revocation list is signed by the authority that has issued the certificate requiring validation

5.6.2 OCSP

The TSP may provide to the third parties with a real-time certificate checking service based on OCSP (Online Certificate Status Protocol). This allows them to verify certificate status immediately.

This service should be available 24 hours a day, 7 days a week.

Use of the OCSP access service will require:

- Checking the URL address contained in the certificate extension “Authority Info Access”.

OCSP responses should conform to RFC6960 and/or RFC5019. OCSP responses should either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

5.7 Network

The TSP should implement a network management procedure according to section 5.2.6 and following requirements indicated by standardization bodies.

It should include all security measures and controls specified for the network devices and also a security policy for the use of networks and network services.

5.8 Infrastructure

The TSP should have an infrastructure that addresses physical and procedural defensive and recovery strategies, countermeasures and resources. This infrastructure should address all the physical and logical issues.

5.8.1 Physical

The site where information is processed should fulfil the following requirements:

- The building housing the information processing facility provides physically security. The exterior walls are solidly built, the site is continuously monitored by video cameras and only duly authorized personnel are allowed access to the site.
- All of the doors and windows are locked and protected to prevent unauthorized access.
- The facility should have a complete physical access control system consisting of:
- Perimeter security which extends from true floor to ceiling to prevent unauthorized access.
- Control over physical access to the facility,
  - Only authorized personnel are allowed access.
  - The rights to access the security area are reviewed and updated periodically.
  - All personnel are required to wear or carry some type of visible identification, and employees are encouraged to question anyone who does not comply with this requirement.
  - Personnel not on the access list who may be working on the site are properly supervised.

For example, a system of closed circuit television which monitors the CA uses in providing its certification services.

5.8.2 Logical

A series of controls are in place in the different components making up the TSP certification service system (CAs, databases, Internet Services, CA Operation and Network Management):

- Operational controls
  - All of the operations procedures are duly documented in the corresponding operations manuals. The TSP maintains a Contingency Plan
  - Tools have been implemented to protect against viruses and malicious codes
  - The equipment is maintained on an on-going basis to ensure uninterrupted availability and integrity
  - A procedure exists for saving, deleting and safely eliminating storage media, removable media and obsolete equipment
- Data exchange. The following data exchanges are encrypted to ensure confidentiality:
  - Transmission of registration data between RAs and the registration database
  - Transmission of pre-registration data
  - Communication between RAs and CAs
- The revocation publication service is available on a 24x7 basis
- Access control
  - Unique user IDs are used in such a way that users are associated with, and can be held responsible for, their actions
  - Rights are assigned according to the principal of providing users with the least amount of system privileges they need to do their jobs

  - Access rights are immediately cancelled whenever users change jobs or leave the organization.
  - The access level assigned to users is revised every three months.
  - System privileges are assigned on a case-by-case basis and terminated once the reason for their assignation is no longer valid.
  - Maintenance password quality guidelines.

5.9 Archiving

The TSP should define and implement the archiving method that complies with what stated in its archiving policy as indicated in section 5.2.2

5.10 Personnel security

The TSP should implement procedures for their personnel regarding security issues and how to proceed. It should define and implement a trusted roles procedure and the tasks to be performed.

A "trusted role" is defined as a person assigned responsibilities than can lead to security problems if not performed satisfactorily, whether accidentally or maliciously.

To ensure that trusted persons perform their corresponding duties properly, the following considerations are addressed:

- The first is that the technology is designed and configured so as to prevent errors and improper conduct
- The second is that duties are distributed among several individuals so that any improper conduct would require the complicity of a number of them

The TSP should have a full definition of all of the roles carried out in the organization. The duties and responsibilities associated with every role are defined, and each has a set of documented procedures which regulate the practical attached to each.

Number of persons required per task

To reinforce system security, more than one person is assigned to each role.

Several individuals may also be assigned to the same role.

Identification and authentication for each role

Trusted roles require verification of identity by secure means; all trusted roles are performed by individuals.

The TSP should have specific documentation giving further details of each role.

5.10.1 Personnel controls

The TSP should implement several controls to check personnel requirements and needs.

Background, qualifications and experience requirement

The TSP employs personnel with the experience and qualifications needed to perform their job.

All personnel with trusted roles should be free from any interests that may affect their impartiality regarding TSP operations.

Training requirements

The TSP should provide its personnel with the training needed to perform their job responsibilities competently and satisfactorily. Personnel training should include the following:

- A copy of the Certification Practice Statement.
- Awareness-raising on security
- Software and hardware operation for each specific role.
- Security procedures for each specific role.
- Management and operation procedures for each specific role.
- Disaster recovery procedure.

The TSP should maintain records of such training and ensure that personnel entrusted to perform such duties satisfactorily.

Retraining frequency and requirements

Any significant change in CA operations should call for a training plan and implementation of the plan should be documented.

Information security incidents

The TSP should have a security incident management plan.

Sanctions for unauthorized actions

The TSP should have an internal disciplinary regime which defines sanctions against personnel

Contracting personnel requirements

The TSP should maintain a policy for contracting personnel and assigning roles and responsibilities.

Documentation supplied to personnel

All personnel with trusted roles should receive:

- A copy of the Certification Practice Statement
- Documentation which defines the obligations and procedures associated with each role
- Personnel also have access to the operations manuals on the various components of the system

6 Conclusions

This document provided an overview of the dedicated means of auditing for TSPs. It discussed specifically the following areas:

- Obligations, warranties and liability of TSPs
- Standards applicable to TSPs and Conformity Assessment Bodies (auditors)
- Methodology of auditing TSPs (off- and on-site)
- TSPs documentation (plans, policies and procedures)
- Implementation of TSPs services

This set of good practices can be used as reference for both, Trust Service Providers (preparing for audits), and Conformity Assessment Bodies (performing audits), in the field of external audits (we consider internal assessments as part of company's risk management procedures, therefore we don't cover this topic here). It focuses on measures that can be taken at organizational level, drawing to norms and standards for technical details.

These guidelines are applicable to the same juridic constituency as the eIDAS Regulation. With the entry of the Regulation into service, national differences in legal or regulatory systems will be abolished.

Examples given in this paper consist relate mainly to certificate providers and certification authorities, however, they apply also to other trust service providers and to all trust services, as defined in the Regulation (including all components of Public Key Infrastructure, electronic seals etc.). Under eIDAS, a Root CA (in the Member States where it exists) can be also considered as a trust service if it fulfills the provisions of the Art. 3.16 (*"service normally provided for remuneration"*).

Definitions

For the purpose of this report, definitions of the Art.3 of the eIDAS Regulation apply. In particular, in this text the following definitions are used:

advanced electronic signature – an electronic signature which meets the requirements set out in Article 26 of the eIDAS Regulation;

authentication – an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;

certificate for electronic signature – an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

certificate for website authentication – an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;

conformity assessment body – a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;

electronic document – any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

electronic identification – the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

electronic identification means – a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

electronic identification scheme – a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

electronic signature – data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

electronic signature creation data – unique data which is used by the signatory to create an electronic signature;

electronic signature creation device – configured software or hardware used to create an electronic signature;

electronic time stamp – data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

qualified certificate for electronic signature – a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS Regulation;

qualified certificate for website authentication – a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

qualified electronic signature – an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

qualified electronic signature creation device – an electronic signature creation device that meets the requirements laid down in Annex II of the eIDAS Regulation;

qualified electronic time stamp – an electronic time stamp which meets the requirements laid down in Article 42 of the eIDAS Regulation;

qualified trust service – a trust service that meets the applicable requirements laid down in eIDAS Regulation;

qualified trust service provider – a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

person identification data – a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

product – hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;

public sector body – a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

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

signatory – a natural person who creates an electronic signature;

trust service – an electronic service normally provided for remuneration which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services;

trust service provider – a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

validation data – data that is used to validate an electronic signature or an electronic seal;

validation – the process of verifying and confirming that an electronic signature or a seal is valid.

References

Legislation and related ENISA papers

[1] 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, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[2] Guidelines for trust service providers – part 1: Security framework, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp1-framework

[3] Guidelines for trust service providers – part 2: Risk assessment, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp2-risk

[4] Guidelines for trust service providers – part 3: Mitigating the impact of security incidents, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp3-incidents

[5] Position Paper of the EP3R Task Forces on Trusted Information Sharing https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tis

Related standards

For the full list of related standards, please refer to section 3 - Standards applicable to TSPs and Conformity Assessment Bodies.

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu