Guidance for the Security requirements applicable to trust service providers

Note on using the guidance: examples are used throughout – they are not normative or exclusive, but there to make the guidance easier to understand as points of reference.

ARTICLE 19.1

Art.19.1 Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

GUIDANCE:

Article 19.1 obliges TSP to setup measures to manage the risk posed to the security of the trust services. Since the Regulation, in absence of Implementation Act, does not provide details about what exactly are *appropriate technical and organisational measures* , rhe appropriate level of security is subject to interpretation. Divergent interpretation of what an appropriate measure is may lead to Inadequate level of security for trust services

- that may cause security breach, if the security level is too low regarding the legal effect of the service,
- that may cause economic issue to a provider that setup unnecessary costly security measures.

The purpose of this guidance is to allow TSP that wants to use convergent set of measures to do so. For that, this guidance provides, when possible, for each type of trust service, a link to the applicable security standard.

- Contextual information about the scope of article 19.1
- A discussion about the different level of security to be taken into account
- For each trust service, a list of applicable measures.

This guidance targets two different objectives:

- automatic legal compliance to eIDAS Regulation for TSPs choosing to follow the guidance;
- maximized the trust of European trust service for users and third parties, thanks to TSPs convergent level of security: If trust service proposes divergent levels of security without adopting a common scale to evaluate the security level, customers of trust service and third parties may have difficulties to assess the security of the offer, and thus, their trust in the services within the scope of eIDAS regulation may be affected in a negative way. This mistrust may lead to difficulties for adoption of Trust Services.

This guidance is written for:

- Qualified Trust Service Provider or Non-Qualified Trusted Service planning to qualify one of their Trust Service. This guidance aims at helping them to setup appropriate and state of art security measures such that their qualification audit will be easier.

- Non-Qualified Trust Service Provider. For them, this guidance aims at helping them to setup appropriate measure to be compliant with Article 19.1.

It is also important to notice that, even if non-qualifed services do not need to be evaluated, they must be compliant Article 19.1.

It also is important to notice that all guidance and proposed measures are provided for ***indicative*** purpose and should be adapted to the specific constraint and environment of each TSP. Depending on the context, the proposed measure may be insufficient, leading to the risk of security breach or may be too strong constraints.

As an example, a signature service may setup stronger security measures depending on the content of the signed data: higher security measures may be setup for signature services that handle contracts involving a high amount of money than the ones handling contracts with lower amount involved.

Therefore, it is recommended that the TSP performs a risk analysis to select the appropriate security measures for its own case.

1. APPLICABLE SCOPE

Article 19.1 specifies that the scope is *Qualified and non-qualified trust service providers.* This specifies that the article is applicable to any provider that delivers at least one trust service as defined in the Regulation (Article 3.16):

- 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;

As mentioned in Art. 19.1, the *measures* to be put in place by the provider shall cover the *security of the trust service they provide*. The obligation to setup measure is not applicable to non-trust service that the provider may distribute or to operation that are not directly related to the trust service.

The Regulation specifies that the measures should be both *technical and organisational*. Therefore, it is important that measures are sufficient in term of strength but that they also cover a sufficient technical and organisational perimeter. For example, an IT system implementing strong access control but implementing no network security will be exposed to attacks.

2. LEVEL OF SECURITY

Article 19.1 specifies that *the level of security is commensurate to the degree of risk*. Trust services may be qualified or not qualified, and these two kinds of services do not have the same legal effects according to eIDAS Regulation. In case of service compromise, the impact is therefore higher for a qualified trust service. Thus, at least two security levels shall be considered:

- a set of security measures for qualified services
- a set of security measures for non-qualified services

However, for an adequate security level, it should be appropriate also to take into account the intended usage of the service:

- the compromise of a TSP that provide a service publicly to a wide number of individual or organisation has more impact than the one of a TSP issuing its service only internally and to a small number of users
- the compromise of a TSP issuing a service to secure critical data has more impact than the one securing non critical data.

Therefore, we propose, in a way to figure out the adapted security level and the corresponding security measures, the following scale for security level

	Non-qualified Service	**Qualified Service**
Public service or critical data	High Security Level	Very High Security Level
Private service and non-critical data	Medium Security Level	High Security Level

This scale is provided throughout the document as indicative guidance as a first evaluation of potentially needed security measures. Therefore, throughout this document, we provide the following table that will help TSP to identifies security measure in line with the security level that would like to achieve.

Security Level	**Proposed security measure**
Very high Security Level	
High Security Level	
Medium Security Level	

3. SECURITY MEASURE REFERENCE STANDARDS

To be compliant with the Regulation, TSPs shall setup appropriate security measures covering both technical and organisational access of the service. Therefore, it is a challenge for TSP to

- Identify all the diiferent technical and organisational aspect to be covered
- Identify, for each aspect, the adequate concrete mesure and level of security.

More over, TSP shall provide evidence that they have set up the appropriate measures regarding to the risk.

A good practice for TSP is to refer to standards that provide security measures that are commonly considered by industry to be appropriate for the specific type of certificates or services described within the standard.

To provide evidence of conformity to the standard, it is recommanded that a conformity assessment should be carried out by a conformity assessment body. This conformity assessment is mandatory for Qualified Services (see Recital 43), but not for non-qualified services. However such assessment process is also recommended to non-qualified TSP who would like to provide evidence that they reach the requirements of Article 19.1 of the Regulation.

The following standards may be used by TSPs who would like to adapt common recognized security measures.

- ETSI TS 119 401/EN 319 401 (General Policy Requirements for Trust Service Providers)
- ETSI TS 119 411/EN 319 411 (Policy and security requirements for Trust Service Providers issuing certificates)
- ETSI TS 119 421/EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Time-Stamps)

- ETSI TS 119 101 (Policy and security requirements for Electronic Signature Creation et Validation)

The following table provides a rationale between the trust services and the standards

	ETSI TS 119 401/EN 319 401	ETSI TS 119 411/EN 319 411	ETSI TS 119 421/ EN 319 421	ETSI TS 119 101
Certificate Issuance Service	X	X		
Time Stamping Service	X		X	
Validation Service	X			X
Signature Preservation Service	X			
Signature Service	X			X
eDelivery Service	X			

4. GENERIC SECURITY MEASURES FOR TRUST SERVICE

ETSI TS 119 401/EN 319 401 provides a generic policy applicable to all Trust Service Provider, qualified and non-qualified. TSP who would like to be in line with industry standard should implement the clause of this standard related to security measures. Since ETSI TS 119 401/EN 319 401 is a generic policy, these recommendations are applicable for any type of trust service.

The applicable clauses are discussed in this section of the guidance.

A. CLAUSE 5 – RISK ASSESSMENT

This clause, related to Risk Assessment, states as follows

> *The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.*
>
> *The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.*
>
> *NOTE: See ISO/IEC 27005 [i.5] for guidance on information security risk management as part of an information security management system.*
>
> *The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment options measures chosen as documented in the information security policy and the trust service practice statement (see clause 6).*
>
> *The risk assessment shall be regularly reviewed and revised.*

When applying that clause, the TSP has *identified, analysed and evaluated trust service risks* and has *selected the appropriate risk treatment measures, taking account of the risk assessment results*. Therefore, by performing the action recommended in this clause, the trust service providers should have taken *appropriate measures to manage the risks posed to the security of the trust services they provide*. Moreover, EN 319 401 Clause 5 specifies that *the risk treatment measures shall ensure that the level of security is commensurate to the degree of risk*. Therefore, *the selected measures* shall *ensure that the level of security is commensurate to the degree of risk, that is a requirement of Article 19.1*.

In addition, Clause 5 states that *the TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment options measures chosen.* This means that the measures shall consider both *technical* (*all security requirements*) and *organisational* (*operational procedures*) level.

To finish with, Clause 5 also states that

> *The risk assessment shall be regularly reviewed and revised.*

By *reviewing* and *revising regularly the Risk assessment*, the TSP is able to integrate *latest technological developments.*

Thus, non-qualified TSPs implementing recommendations of EN 319 401 Clause 5 for each service they provide, may be considered to match the definition of article 19.1, since *they take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.*

We provide in the following table indicative proposition on how a TSP may implement that clause depending on the targeted security level. TSP shall adopt these propositions depending on their proper context.

Security Level	**Proposed security measures**

Very high Security Level	- Risk assessment shall cover **all aspect of the trusted service** (both technical and non-technical)
	- Risk assessment shall follow the methodology recommended by the national supervisory body, or if no specific methodology is proposed, shall follow ISO/IEC 27005 or equivalent methodology
	- Risk assessment shall be formally validated by Management
	- Risk assessment shall be reviewed
	  ○ At least once a year
	  ○ Before any important internal change is performed on the service
	  ○ At least in **two months** after any important external change.

High Security Level	- Risk assessment shall cover a**ll aspect of the trusted service** (both technical and non-technical)
	- Risk assessment shall follow the methodology recommended by the national supervisory body, or if no specific methodology is proposed, shall follow ISO/IEC 27005 or equivalent methodology
	- Risk assessment shall be formally validated by Management
	- Risk assessment shall be reviewed
	  ○ At least once a year
	  ○ **Before** any important internal change is performed on the service
	  ○ At least in **4 months** after any important external change.

Medium Security Level	- Risk assessment shall cover all **critical assets** of the trusted service and shall cover both technical and non-technical aspects

	- **Risk assessment shall follow any methodology at long as the methodology identifies assets, threat and counter-measures**.
	- Risk assessment shall be reviewed
	  o At least every 3 years
	  o **When** any important internal change is performed on the service
	  o At least in 6 **months** after any important external change

B. GENERALITIES ON THE OTHER CLAUSES

It is important to notice that all trusted services have practices in common. For example, for their operations, they need to ensure confidentiality, integrity and availability of secrets (such as private keys), if they handle any secret. . They also need to set up traceability of operations. Therefore, since they may have common practices and common assets to protect, they should have common also common threats and common security measures to set up for covering these threats.

ETSI TS 119 401/EN 319 401 provides a set of security measures considered by industry to be standard answers to common threat of Trusted Services. By adopting these measures, a TSP will more easily be able to demonstrate that he has set up appropriate security measures, since these measures have already been considered as efficient by the industry. Of course, a TSP may choose to not follow the security measures provided in this standard and set up is own set of measures. , However, this may lead to divergent interpretations between TSPs of the kind of Risk assessment to perform, and therefore that may leads to*, in fine*, to divergent levels of security between the TSPs. A heterogeneous level of security for similar services may lead to difficulties for trusted service adoption and European digital exchange. Therefore, it is recommended that TSPs and Supervisory bodies both adopt a common framework of security measures.

Therefore this document identifies:

- the clauses describing security measures that may be applied, and
- for a given security level identified in §2(Level of Security, concrete examples explaining, how the guidance may be implemented.

Clauses identified in ETSI TS 119 401/EN 319 401 provide guidance for security measures. The list of these clauses is provided in the following table:

Clause Number	Title	Clause Number	Title
Clause 6.3	Information security Policy	Clause 7.2	Human Resources
Clause 7.3	Asset Management	Clause 7.4	Access control
Clause 7.5	Cryptographic Control	Clause 7.6	Physical and environmental security
Clause 7.7	Operation Security	Clause 7.8	Network Security
Clause 7.9	Incident Management	Clause 7.10	Collection of evidence
Clause 7.11	Business continuity management	Clause 7.12	TSP termination and termination plan.

In the next section, we discuss the content of each of these clauses.

C. CLAUSE 6.3 - INFORMATION SECURITY POLICY

CLAUSE DISCUSSION

This clause proposes to Document information security in a policy. Having such a policy is a good practice since this allows:

- To share a common view in the organization on how security shall be managed.
- To provide a reference for controlling purposes if security measures identified in the policy have been set up.
- To have an overview of the security allowing to ensure that all security aspect are covered.

It is important to notice that not having information policy may lead to:

- The risk that security measures and practices may not be commonly understood within the organization and therefore security measures may not be implemented at all or may not be well-implemented or may be implemented in a heterogeneous way in different part of the organization, since they have been understood in a different way.
- The rick of a lack of global view of the security. That may lead to an incomplete coverage of the security perimeter. For example, logical access control may be well implemented by physical access control have not been addressed.
- Lack of capacity to compare low level measures with high level requirements.

Such events may leads to a state of where inappropriate *technical and organizationalmeasures to manage the risks* are taken and thus, *in fine*, to a non-compliance with Art 19.1 of the Regulation.

IMPLEMENTATION GUIDANCE

We provide in this section detailed implementation guidance for this clause in the aim of helping TSP, who would like to implement it. We propose security measures for each element of the clause.

Clause 6.3 states that:

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

Security Level	Proposed security measures
Very high Security Level	The Information Security Policy shall be formally approved by management with written or electronic signature of management representative.
High Security Level	
Medium Security Level	

> *a) A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP facilities, systems and information assets providing the services.*
>
> *The TSP shall publish and communicate this information security policy to all employees who are impacted byit.*
>
> *NOTE 1: See clause 5.1.1 of ISO/IEC 27002:2013 [i.3] for guidance.*

Security Level	Proposed security measures
Very high Security Level	Each employee shall have an access to written or electronic documentation for each operational procedure he may have to perform. He or she shall also have access to general policies such as, for example, applicable CP/CPS for a CA. Documentation shall be communicated through a permanent media. Example of permanent media may include : - printed documentation, - access to a web repository or wiki, - electronic document provided by email. **Each employee shall be personally notified of any change in the documentation.**
High Security Level	
Medium Security Level	Each employee shall have an access to written or electronic documentation for each operational procedure he may have to perform. He or she shall also have access to general policies such as, for example, applicable CP/CPS for a CA. Documentation shall be communicated through a permanent media. Example of permanent media may include : - printed documentation, - access to a web repository or wiki, - electronic document provided by email.

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

Security Level	Proposed security measures
Very high Security Level	No specific guidance for this point.
High Security Level	
Medium Security Level	

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

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

Security Level	Proposed security measures
Very high Security Level	We recommend to apply the CAB Forum recommendation: Review of the configuration of all critical trusted service subsystem shall be performed on at least a **weekly** basis to determine whether any changes violated the security policies. For example, for a TSP issuing certificate, the configurations to be reviewed include: - Issuing Systems, - Certificate Management Systems, - Security Support Systems, and - Front-End / Internal-Support Systems
High Security Level	
Medium Security Level	Same recommendations on a **monthly** basis.

> *d) A TSP's management security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP facilities, systems and information assets providing the services.*
>
> *NOTE 3: See clause 5.1.1 of ISO/IEC 27002:2013 [i.3] for guidance.*

Security Level	Proposed security measures
Very high Security Level	No specific guidance other than the ones provided within clause 5.1.1 of ISO/IEC 27002:2013.
High Security Level	
Medium Security Level	

D. CLAUSE 7 - MANAGEMENT AND OPERATION

These clauses address the organisational part required by Art. 19.1.

CLAUSE 7.2 - HUMAN RESOURCES

CLAUSE DISCUSSION

Even if trusted services security may involve high technological software and hardware, they are operated by human being. Human beings are perfectible by nature and may unintentionally do errors or may intentionally provoke faults.

Therefore, *adequate organizational measures* should include security measures regarding human resources.

IMPLEMENTATION GUIDANCE

Regarding human resources, the clause indicates that

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

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

Trusted services security and trust cannot be reached without a strong involvement of employees and contractors in the security requirements. This shall be based on:

- Responsibility of employees and contractors
- Appropriate employees and contractors selection process.

Clause 6.1.1 of ISO ISO/IEC 27002:2013 provides guidance regarding Responsibilities of employees.

Clause 7 of ISO ISO/IEC 27002:2013 provides guidance for employees selection.

RESPONSIBILITIES OF EMPLOYEES AND CONTRACTORS

ISO/IEC 27002:2013 states that

> *Functions and assets shall be identified.*
>
> *Responsibilities shall be defined and attributed.*
>
> *Responsibilities shall be documented*
>
> *Employee responsible for a function or an asset shall be competent*

It is important to notice that:

- A TSP that implement our guidance on Risk Assessment (see Clause 5 – Risk Assessment) shall be compliant with the first recommendation
- A TSP applying our recommendations of this section concerning "TRAINING AND AWARENESS" and "EMPLOYEES SELECTION" of this chapter shall have employees covering the competency requirement.

Therefore, we need security measures to cover the following:

> *Responsibilities shall be defined and attributed.*
>
> *Responsibilities shall be documented*

We propose the following examples to cover these remaining requirements

Security Level	**Proposed security measures**
Very high Security Level	The TSP documents an inventory of roles. A role description includes a list of responsibilities. Each responsibility shall be clearly documented. For each role, an inventory shall map the role to the person or the group of person who is responsible for this role. Every person having responsibilities in Trusted Service Function shall accept formally the responsibilities in a way such that non-repudiation is not possible (e.g. a written engagement)
High Security Level	
Medium Security Level	

EMPLOYEES SELECTION

ISO/IEC 27002:2013 clause 7, proposes the following security measures:

Background checks shall be performed before selection of employees

Specific contractual clauses regarding the responsibilities

Security guidance follow up by employee shall be supported by Management

Adequate training of employees shall be performed

Disciplinary sanctions

Contract shall include responsibilities that are permanent

The reader can refer to ISO/IEC 27002:2013 clause 7 for a detailed description of these recommendations. We provide, for each level, example of what could be done according to the security level.

BACKGROUND CHECKS

Notice that all checks shall be performed accordingly with the local laws and regulations. Examples of background checks adapted to the security level are as follows:

Security Level	Proposed security measures
Very high Security Level	- At least the **three** last positions of the candidate are verified in an independent way. This may be done by research on internet, call to employee, third party reference, *etc.*) - At least **three** references shall be provided by the candidate. **Two** at least shall be professional ones - The candidate shall provide copy of **all** diplomas claimed in the C.V. - The candidate shall present his or her **original ID document** and a copy is kept by the TSP. - The candidate shall provide criminal record. - Competency shall be asserted by **two technical** interviews - Background checks process is documented and specifies the responsibilities in the process. - TSP keeps records of all elements of the background check process.
High Security Level	- At least the **two** last positions of the candidate are verified in an independent way. This may be done by research on internet, call to employee, third party reference, *etc.*) - At least **two** references shall be provided by the candidate. **One** at least shall be professional - The candidate shall provide copy of **last (or higher degree**) diplomas claimed in the C.V. - The candidate shall present his or her **original ID document** and a copy is kept by the TSP. - The candidate shall provide criminal record. - Competency shall be asserted by **one technical** interviews - Background checks process is documented and specifies the responsibilities in the process. TSP keeps records of all elements of the background check process
Medium Security Level	- At least **the last position** of the candidate is verified in an independent way. This may be done by research on internet, call to employee, third party reference, etc.) - At least **one** reference shall be provided by the candidate. **This reference** shall be professional - The candidate shall provide copy of **last (or higher degree)**

	diplomas claimed in the C.V. - The candidate shall present a **copy of ID document** that shall kept by the TSP. - The candidate shall provide criminal record. - Competency shall be asserted by **one technical** interview - Background check process is documented and specifies the responsibilities within the process. - TSP keeps records of all elements of the background check.

SPECIFIC CONTRACTUAL CLAUSES REGARDING THE RESPONSIBILITIES

Within contracts (with employees and contractors), TSP shall clearly states the respective responsabilities.

Security Level	Proposed security measures
Very high Security Level High Security Level Medium Security Level	All employees and contractors shall sign a confidentiality form on an individual basis before access to confidential information is granted. This form shall include: - Information related to legal responsibilities and the rights of the employee or contractor. - Responsibilities related to the classification of information and asset management - Responsibilities of employees and contractors - Actions that may be performed by TSP if confidentiality measures have not been followed by employees or contractors Responsibilities regarding information security shall be specified before entering into contractual relationship. This may be performed for example by: - Specifying security responsibilities in job ad or job description - Specifying security requirements and responsibilities in RFP or tender for future contractors. Details of the expected behaviour and the rules to be followed may be provided by reference to an IT charter, security policy and/or internal rules documentation.

SECURITY GUIDANCE SUPPORT BY MANAGEMENT

Management shall support security. This may be performed as follows:

Security Level	Proposed security measures
Very high Security Level High Security Level Medium Security Level	- Management shall ensure that employees are correctly informed of their roles and responsibilities before accessing to confidential information. This may be reached by management by setting up an information security step during the procedure. - Management shall ensure that employees are aware of general security guidance. This may be reached by the diffusion of security guidance document and/or by a dedicated presentation with mandatory participation of employees - Management shall provide incentive to respect security measures. This may be performed, for example, by adding criteria on compliance to the security in the annual employee evaluation or by adding KPI related to security in management follow-up. - Management shall support staff awareness regarding information security. This may be performed by specific training of employees on an annual basis for example

	- Management shall ensure that employees permanently follow their initial confidentiality agreement. This may be performed by a reminder of the conditions of the agreement on an annual basis - Management shall include regular training to ensure that employees maintain an adequate level of competency (see next section) - Management shall provide an anonymous way allowing employees to report security issues or incidents. - Management shall support and follow security guidance. This may be performed by including management practices within the scope of internal audits.

TRAINING AND AWARENESS

Program aiming at developing information security awareness of employees should be performed.

Security Level	Proposed security measures
Very high Security Level	- Every employee should follow a security awareness session **every year**. - Content of the security awareness actions (training, information) shall be in line with security policy. Therefore, the content shall be reviewed after every major change in the security policy and at **least every year**.
High Security Level	- Every employee should follow a security awareness session **every two years**. - Content of the security awareness actions (training, information) shall be in line with security policy. Therefore, the content shall be reviewed after every major change in the security policy and at **least every two years**.
Medium Security Level	- Every employee should follow a security awareness session **every three years**. - Content of the security awareness actions (training, information) shall be in line with security policy. Therefore, the content shall be reviewed after every major change in the security policy and at **least every three years**.

DISCIPLINARY PROCESS

ISO/IEC 27002:2013 clause 7.2 proposes guidance regarding disciplinary process.

Security Level	Proposed security measures
Very high Security Level	All employees shall be aware of the disciplinary process and the consequences of their action. Therefore, disciplinary process should be documented and shall be provided to employee in an accessible and permanent way. This may be done, for example, by distributing of paper copy of the documentation to each employee or by dedicating a specific webpage on the intranet.
High Security Level	
Medium Security Level	

END OF CONTRACT

ISO/IEC 27002:2013 clause 7.3 proposes guidance regarding the end of contract between employees and TSP and/or between contractor and TSP. In particular, contracts shall clearly identify the clause that remain valid after the end of the contract (e.g. clause related to the confidentiality of information).

Security Level	Proposed security measures
Very high Security Level	No additional specific security measure.
High Security Level	
Medium Security Level	

CLAUSE 7.3 - ASSET MANAGEMENT

CLAUSE DISCUSSION

Asset management is a fundamental element of organizational security. Even if trusted services security may use highly secured assets, improper management of these assets may lead to the theft, lost or compromise of sensible data. For example, improper management of the end of life of media used for the operation of the Trusted Service may leads to the disclosure of the sensible information contained in the media.

Therefore, *adequate organizational measures* should include security measures regarding asset management.

IMPLEMENTATION GUIDANCE

> *The TSP shall ensure an appropriate level of protection of its assets including information assets.*
>
> *NOTE 1: See clause 8 of ISO/IEC 27002:2013 [i.3] for guidance.*

Clause 8 of ISO/IEC 27002:2013 states that the following measures should be done

- Assets shall be managed
- Information shall be classified
- Media shall be manipulated in a secure way

The reader should follow the guidance provided in of ISO/IEC 27002:2013. We provide in this document specific guidance regarding inventory and media handling

> *In particular, the TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment.*
>
> *NOTE 2: See clause 8.1.1 of ISO/IEC 27002:2013 [i.3] for guidance.*

Measure to be set up may include the identification of assets included in the information life-cycle. We provide propositions of security measures for each identified security level.

Security Level	Proposed security measures
Very high Security Level	- If the identification of assets has not been performed during the risk assessment, identification of assets involved in the information

	life cycle shall be performed. - An inventory of **all assets** involved in the information life cycle shall be performed. - Inventory shall be updated **immediately** after any action. - All assets or classes of asset shall have an identified owner. Ownership of critical assets such as HSM or administrative smartcards shall be accepted by employees through a written agreement or equivalent (for example, electronically signed agreement). - Inventory of critical assets shall be checked on a **monthly** basis. - Inventory of non-critical assets shall be checked on a yearly basis.
High Security Level	- If the identification of assets has not been performed during the risk assessment, identification of assets involved in the information life cycle shall be performed. - An inventory of **all assets** involved in the information life cycle shall be performed - Inventory of critical assets shall be updated **at least 48h** after any action. - Inventory of non-critical assets shall be updated one week maximum after any action and preferably immediately - All assets or classes of asset shall have an identified owner. Ownership of critical assets such as HSM or administrative smartcards shall be accepted by employee through a written agreement or equivalent (for example, electronically signed agreement). - Inventory of critical assets shall be checked on a **monthly** basis. - Inventory of non-critical assets shall be checked on a yearly basis.
Medium Security Level	- If the identification of assets has not been performed during the risk assessment, identification of assets involved in the information life cycle shall be performed. - An inventory of **all assets containing confidential information** shall be performed - Inventory shall be updated **at least 72h** after any action. - Inventory of non-critical asset shall be updated at least one week after any action - All assets or classes of assets shall have an identified owner. Ownership of critical assets such as HSM or administrative smartcards shall be accepted by employee through a written agreement. - Inventory of critical assets shall be checked on a **monthly** basis.

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

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

All media containing sensitive information shall be manipulated in a secure way. This includes

- Removable media management
- End of life of assets
- Transport of assets

We provide examples of security measures.

REMOVABLE MEDIA MANAGEMENT

TSP shall setup security measures such that media are managed in a secure way.

Security Level	Proposed security measures
Very high Security Level	- Removable media used in production **shall not be re-used** in another perimeter and shall be destroyed if not used anymore. - Critical media shall be kept in a safe under dual control - Non critical media shall be kept in secured premises with physical access control. - All sensible information shall be stored encrypted - When possible removable media shall be renewed, for example every three years and multiple copies on several media shall be performed - Inventory of removable media shall be done - Use and access to removable media containing sensitive information shall be documented
High Security Level	- Removable media used in production **shall not be re-used** in another perimeter and shall be destroyed if not used anymore. - Critical media shall be kept in a safe under the exclusive control of their owners. - Non critical media shall be kept in secured premises with access control. - All sensible information shall be stored encrypted - When possible, removable media shall be renewed, for example every three years and multiple copies on several media shall be performed - Inventory of removable media shall be done - Use and access to removable media containing sensitive information shall be documented
Medium Security Level	- Removable media **shall be processed such that sensitive information are not accessible** before been used in another perimeter and destroyed if no secured erasing process is available. - **If a media is used outside the perimeter, an authorization shall be given and traceability of the authorization shall be kept.** - Critical media shall be kept in a safe. - Non critical media shall be kept in secured premises with access control. - All sensible information shall be stored encrypted or at least with adequate access control. - When possible, removable media shall be renewed, for example every three years and multiple copies on several media shall be performed - Inventory of removable media shall be done - Use and access to removable media containing sensitive - information shall be documented information shall be documented

END OF LIFE MANAGEMENT

TSP shall setup security measures such that end of life assets is not a source of data leakage

Security Level	Proposed security measures
Very high Security Level High Security Level Medium Security Level	- All HSM shall be zeroized and shall been physically destroyed according to vendor recommendations. - All smartcards shall be shredded with an accurate method (for example, a shredder meeting the requirements of NSA/CSS Policy Manual 9-12) - All media such as DVD shall be shredded - All hard disk shall be erased before being destroyed by accurate process. - All media with inadequate zeroization shall be kept in a safe instead of been destroyed or trashed. - Organization handling media destruction shall be carefully selected and shall provide state of the art destruction method - Destruction of assets containing sensitive data shall be performed in front of the owner of the asset and at least a witness.

TRANSPORT OF ASSETS

TSP shall setup security measures such that assets are not altered during the transport

Security Level	Proposed security measures
Very high Security Level	- Sensitive assets shall only be transported by trusted third parties carefully selected or by person in trusted role. - TSP shall use temper evidence mechanism, such as sealed envelope with unique identification number, every time a sensible media is transported - Temper evidence shall be before and after transportation checked by trusted role in **dual control** - When sensitive assets are transported by third parties, identification of third party shall be performed - Traceability elements shall be kept
High Security Level	- Sensitive assets shall only be transported by trusted third parties carefully selected or by person in trusted role. - TSP shall use temper evidence mechanism, such as sealed envelope with unique identification number, every time a sensible media is transported - Temper evidence shall be before and after transportation checked by trusted role in **dual control** - When sensitive assets are transported by third parties, identification of third party shall be performed - Traceability elements shall be kept
Medium Security Level	- Sensitive assets shall only be transported by trusted third parties carefully selected or by person in trusted role. - TSP shall use temper evidence mechanism, such as sealed envelope with unique identification number, every time a sensible media is transported - Temper evidence shall be before and after transportation checked by **a person in trusted role** - When sensitive assets are transported by third parties,

	identification of third party shall be performed - Traceability elements shall be kept

CLAUSE 7.4 - ACCESS CONTROL

CLAUSE DISCUSSION

Access control rules shall be set to ensure availability, confidentiality and integrity of the sensible data manipulated by a TSP. Without adequate access control rules, sensible data may be access, modified or deleted by unauthorized persons.

Therefore, *adequate technical and organizational measures* should include appropriate access control rules and proper implementation.

IMPLEMENTATION GUIDANCE

Clause 7.4 states that:

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

This particularly clause applies :

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

Security Level	Proposed security measures
Very high Security Level High Security Level Medium Security Level	This can be done, when possible, by a role-based user management, *e.g.* - by defining at least the following three roles: operators, administrators and auditors - by assigning adequate privileges to each role - by assigning the adequate role to users It is recommended to perform access removal as follows: - first by deleting privileges (or role) assigned to the user - second by deactivating the user.

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

Security Level	Proposed security measures

Very high Security Level	No specific recommendation
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	- Nominative accounts are used each time is possible - Authentication is performed with certificates stored within secured device (e.g. with a qualified certificate) each time it is possible, with software certificate or strong password otherwise.
High Security Level	- Nominative accounts are used each time is possible Authentication is performed with certificates stored within secured device (e.g. with a qualified certificate) or with software certificate otherwise.
Medium Security Level	- Nominative accounts are used each time is possible Authentication is performed with software certificate or strong password otherwise.

e) TSP personnel shall be accountable for their activities

Security Level	Proposed security measures
Very high Security Level	This may be performed by retaining event logs. It is recommended that personnel performing actions shall not be able to access to logs. This may be performed by an electronic seal of the logs or access restriction rules.
High Security Level	
Medium Security Level	

CLAUSE 7.5 – CRYPTOGRAPHIC CONTROLS

CLAUSE DISCUSSION

Cryptographic keys are a powerful tool to ensure security property such as confidentiality (thanks to encryption) or integrity and non-repudiation (thanks to signature). Most trust services, such as PKI services, should be based on such cryptographic mechanisms. However, if appropriate controls are not taken to protect the use these cryptographic keys, the security of the overall service may be jeopardized.

Therefore, appropriate technical and organisational security measures shall implement such controls.

IMPLEMENTATION GUIDANCE

Clause 7.5 states

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

Security Level	Proposed security measures
Very high Security Level	It is recommended to protect keys by a method involving at least a dual control and a two factor authentication. Control based on a quorum of smartcards (typically 2 cards in a set of 5) is appropriate to cover both the need of dual control and the need of availability of the operators.
High Security Level	
Medium Security Level	

CLAUSE 7.6 - PHYSICAL AND ENVIRONMENTAL SECURITY

CLAUSE DISCUSSION

TSP operated in a non-secured environment will not provide adequate security level. For example, without adequate physical measures, assets may be physically accessed by attackers, may be theft or destroyed.

Therefore, *appropriate technical and organizational security measures* shall take into account physical and environmental security.

IMPLEMENTATION GUIDANCE

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

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

In particular:

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

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

We provide examples of security level

Security Level	Proposed security measures
Very high Security Level	Access to the premises shall be based on two factors authentication. Components shall be operated in a private area (It is not mandatory that the TSP owned to area, it may be a private room rented in a data-center) Highly critical components such as root CA shall be accessed with dual control. Identification of the personal accessing to the premises shall be performed

	(e.g. by ID document control)
High Security Level	Access to the premises shall be based on two factors authentication. Components shall be operated in a private area. Highly critical components such as root CA shall be accessed with dual control.
Medium Security Level	Access to the premises shall be based on a single-factor and a formal identification.

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

Security Level	Proposed security measures
Very high Security Level	Security measures shall be setup against power disruption, flood and fire.
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	Only authorized personal shall be able to remove elements such as server from processing facilities.
High Security Level	
Medium Security Level	

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

We propose, as an example, the following security measures:

Security Level	Proposed security measures
Very high Security Level	Physical protection against intrusion includes - Closed computer rack - Protection grid on walls, ceiling and floor - Minimal distance between computer rack and walls - Dedicated access mechanism on area entries - Video camera with automatic movement detection - Several points of control before accessing the premises.
High Security Level	
Medium Security Level	

CLAUSE 7.7 - OPERATION SECURITY

IMPLEMENTATION GUIDANCE

> *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.*

Trustworthy systems and products are discussed in our guidance regarding Article 24.

CLAUSE 7.8 - NETWORK SECURITY

CLAUSE DISCUSSION

TSP exchange sensible data through network (that may be internal network or internet). If network connections are not secured, sensible data may be disclosed or modified, leading to security breaches.

Therefore, *appropriate technical and organizational security measures* shall take into account network security.

IMPLEMENTATION GUIDANCE

> *The TSP shall protect its network and systems from attack.*

The following security measures are recommended

Security Level	Proposed security measures
Very high Security Level	Most critical systems such a Root CA shall be put offline. All systems shall be protected against network attacks, this includes measures like: - Use of firewall with adequate configurations - Separation of the components in dedicated VLAN - Application of security patches on servers - Minimal external exposition of services. The use of certified network devices is recommended. Authentication and Protection (integrity/confidentiality) of communication between components is recommended with protocols such as TLS/SSL.
High Security Level	
Medium Security Level	

CLAUSE 7.9 - INCIDENT MANAGEMENT

CLAUSE DISCUSSION

Even if appropriate measures are setup, TSP may encounter incidents. Impacts of incident are minimized if TSP is able to handle them quickly and appropriately. On the contrary, if an incident is not managed or detected, that may leads to bigger impact than the initial one. As an example, if a TSP detect that a backup of the cryptographic key is unusable (this can be caused by the destruction of the storing media of the key), then

- If the TSP immediately respond to the incident by creating a new backup, the impact is minimized.
- If the TSP doesn't respond, the next incident may lead to the loss of the key, since there is no backup anymore.

Therefore, *appropriate technical and organizational security measures* shall take into account security measures ensuring efficient incident management.

IMPLEMENTATION GUIDANCE

> *System activities concerning access to IT systems, user of ITsystems, and service requests shall be monitored. In particular:*
>
> *a) Monitoring activities should take account of the sensitivity of any information collected or analyzed.*

Security Level	Proposed security measures
Very high Security Level	If monitoring provided access to sensitive information, security measures shall be taken to protect this information.
High Security Level	
Medium Security Level	

> *b) Abnormal system activities that indicate a potential security violation, including intrusion into the TSP network, shall be detected and reported as alarms.*
>
> *NOTE 1: Abnormal network system activities can comprise (external) network scans or packet drops.*

Security Level	Proposed security measures
Very high Security Level	This may be done by the use of Intrusion Detection Systems.
High Security Level	
Medium Security Level	

> *c) The TSP IT systems shall monitor the following events:*
>
> *i) Start-up and shutdown of the logging functions; and*
>
> *ii) Availability and utilization of needed services with the TSP network.*

Security Level	Proposed security measures
Very high Security Level	No specific recommendation
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	TSP shall - define who is responsible for processing the alert and shall define the escalation procedure - setup incident response plan
High Security Level	
Medium Security Level	

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

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

Security Level	Proposed security measures
Very high Security Level	No specific additional recommendation
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	TSP shall setup a written procedure to identity impacted users and to notify them. This procedure may be included in a communication plan.
High Security Level	
Medium Security Level	

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

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

We propose the

Security Level	Proposed security measures
Very high Security Level	- Audit log monitoring and automatic anomaly detection shall be performed in a continuous way - Manual review shall be performed **without delay** when an anomaly is detected - Correlation of Audit log and review shall be performed in an automatic way and at least **once a week**
High Security Level	- Audit log monitoring and automatic anomaly detection shall be performed in a continuous way - Manual review shall be performed **without delay** when an anomaly is detected - Correlation of Audit log review shall be performed in an automatic way and at least **once a week**
Medium Security Level	- Audit log monitoring and automatic anomaly detection shall be performed in a continuous way - Manual review shall be performed **without delay** when an anomaly is detected - Correlation of Audit log review shall be performed in an automatic or manual way and **at least once a month**

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

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

Security Level	Proposed security measures
Very high Security Level	No specific additional recommendation
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	No specific additional recommendation
High Security Level	
Medium Security Level	

CLAUSE 7.10 - COLLECTION OF EVIDENCE

CLAUSE DISCUSSION

In case of complain or in case of incident, a TSP shall be able to investigate and to provide

- Evidences that operations have been performed normally or
- Elements to understand an inappropriate behaviour have been identified. That allows the TSP to set up an appropriate response.

In both cases, evidences shall be collected.

Therefore, *appropriate technical and organizational security measures* shall take into account security measures ensuring collections of evidence.

IMPLEMENTATION GUIDANCE

> *The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.*
>
> *In particular:*
>
> *a) The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.*

Security Level	Proposed security measures
Very high Security Level	Integrity and confidentiality may be reached by appropriate access control rules. eSignature, eSeal or timestamping of the archived may be used to achieve evidence of integrity. Various solution may be used for archiving including: - Writing archive on read-only physical media stored in a safe - Storing archive on server with appropriate physical and logical security measures.
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	- No specific recommendation

High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	TSP shall ensure that archivse are appropriately classified (e.g. per date and per server) such that evidence shall be easily find and retrieved.
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	It is recommended to synchronize all servers with the same NTP server, such that time drifting inconstancies do not appear when correlating the logs. Offline server should be synchronized with precise clock system such as time-server to avoid time drifting of the servers, since thay cannot be synchronized with an external OTP server.
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	TSP shall specify the retention period and setup a procedure to erase the record at the end of the retention period.
High Security Level	
Medium Security Level	

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

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

Security Level	Proposed security measures
Very high Security Level	Events logs shall be collected and saved on a regular basis and if possible immediately after their generation. Externalization and Archiving shall be performed at least once a month.
High Security Level	
Medium Security Level	

CLAUSE 7.11 - BUSINESS CONTINUITY MANAGEMENT

CLAUSE DISCUSSION

Security of TSP assets and services shall be ensured even in case of abnormal state of operation, i.e. in case of incident or in case of a disaster.

Therefore, *appropriate technical and organizational security measures* shall include Business Continuity management plan.

IMPLEMENTATION GUIDANCE

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

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

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

Security Level	Proposed security measures
Very high Security Level	TSP shall set up Business Continuity Plan and Business Recovery Plan. The plan has to be documented and shall be tested completely **every year** Report of the execution of the plan shall be produced and anomaly shall be corrected
High Security Level	TSP shall set up Business Continuity Plan and Business Recovery Plan. The plan has to be documented and shall be tested completely **every 2 years** Report of the execution of the plan shall be produced and anomaly shall be corrected
Medium Security Level	TSP shall set up Business Continuity Plan and Business Recovery Plan. The plan has to be documented and shall be tested completely **every 3 years** Report of the execution of the plan shall be produced and anomaly shall be corrected

CLAUSE 7.12 - TSP TERMINATION AND TERMINATION PLANS

CLAUSE DISCUSSION

If a TSP decides to stop a trusted service, this end of service shall not induce security impact on the Trust service users, former users, and Third Parties. TSP shall also, at least, minimize that impact of the termination. For example, the end of life of a signature service shall not induce the invalidation of all the signatures produced by this signature service.

Therefore, *appropriate technical and organisational security measures* shall include Termination plan.

IMPLEMENTATION GUIDANCE

> *Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.*
>
> *In particular:*
>
> *a) The TSP shall have an up-to-date termination plan.*
>
> *b) Before the TSP terminates its services at least the following procedures apply:*
>
> *i) the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSP. In addition, this information shall be made available to other relying parties;*

Security Level	Proposed security measures
Very high Security Level	TSP shall document the termination plan. It is recommended that this termination plan include a communication plan. Provision shall be made to execute such a plan.
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	No specific recommendation
High Security Level	

Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	If an obligation transfer is plan Third parties shall be identified and provision and/or pre-contracting shall be done to ensure that the transfer will be performed.
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	TSP shall document such destruction procedure in the termination plan.
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	No specific requirement
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	See comment above on provision
High Security Level	

Medium Security Level	

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

i) notification of affected entities; and

ii) transferring the TSP obligations to other parties.

Security Level	Proposed security measures
Very high Security Level	See comment above on provision
High Security Level	
Medium Security Level	

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

Security Level	Proposed security measures
Very high Security Level	This may be performed by the provision or the pre-payment of a webserver and domain name hosted by third parties. The period shall at least cover the expiration of the last issued certificate.
High Security Level	
Medium Security Level	

5. SPECIFIC MEASURES FOR TRUSTED SERVICES ISSUING CERTIFICATES

The ETSI EN 319 411-1 provides a list of requirements for TSP issuing certificates. In this document, specific security measures concerning certificate issuance services in the clauses 6.4, 6.5 and 7.1.

A TSP issuing certificates that would like to meet state of the art security measures may follow these recommendations. We provide the details of these three clauses.

A. CLAUSE 6.4 - FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This clause, in addition of security requirements provided in ETSI EN 319 401 (see Section 4 of this document) specifies specific requirements covering the following area:

- Physical Security Controls
- Procedure Controls
- Personnel Controls
- Audit logging procedure
- Record Archival
- Compromise and disaster recovery

- Certification Authority or Registration Authority termination

PHYSICAL SECURITY CONTROLS

ETSI EN 319 411-1 states that

> *Certificate generation and revocation management*
>
> *a) The facilities concerned with certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems for data.*

This means that Certificate generation and revocation functions, for an adequate protection, should be operated in conditions such that it meet the requirement described in clause §7.6 of ETSI TS 119 401/EN 319 401 with the guidance provided in this document (see 4.D)

> *b) Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exit shall be logged.*

No specific guidance for this point. This may be simply done by a seggregation of duty.

> *c) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.*

This may be achieved with, for example, a private area rented within a data-center.

> *d) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The TSP's physical and environmental security policy for systems concerned with certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.*

No specific Recommendations regarding this point. TSP should verify that housing system have state of the art measures in place. Elements such as proven compliance to ISO 27001 or PCI-DSS/PCI-PIN may be strong evidence of compliance to that point.

> *e) Controls shall be implemented to protect against equipment, information, media and software relating to the TSP services being taken off-site without authorization.*

This requirement may be fulfilled by setting up a list of authorized person allowed to take-off media.

> *f) Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.*

No specific requirements.

> *g) Root CA keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates.*

Common practices for isolating root CAs may include:

- operating root CAs offline;
- using separate hardware for root CAs and operational subCAs.

PROCEDURE CONTROLS

ETSI EN 319 411-1 states that

> *The requirements identified in ETSI EN 319 401 [8], clause 7.4, items b), c), d) and e) shall apply.*
>
> *In addition the following particular requirements apply:*

See Section D.4 for guidance regarding ETSI EN 319 401 clause 7.4.

> *NOTE: With regards general to requirement "Sensitive data shall be protected" [8], Sensitive data includes registration information.*

No specific recommendations.

> ***Certificate generation***
>
> *a) The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.*

The following security measures may be adopted by TSP

Security Level	Proposed security measures
Very high Security Level	Authentication with qualified certificate
High Security Level	Authentication with qualified certificate
Medium Security Level	Authentication with certificate held on hardware token.

> ***Dissemination***
>
> *b) Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.*

TSP shall be specifically careful regarding data storing system such as databases.

> ***Certificate Revocation status***

> *c) Revocation status application shall enforce access control on attempts to modify revocation status information.*

TSP shall be specifically careful regarding :

- The protection of the CRL signing key. It is recommended to have the same security level that the certificate issuance signing key and adequate activation mechanism
- The system storig the revocation status information (e.g. Databases)

PERSONNEL CONTROLS

ETSI EN 319 411-1 states that

> *The requirements identified in ETSI EN 319 401 [8], clause 7.2 shall apply:*
>
> *a) In addition to the trusted roles identified in ETSI EN 319 401 [8], 7.2 item g), the trusted roles, of the registration and revocation officers responsibilities as defined in CEN TS 419 261 [i.9] shall be supported.*
>
> *b) [PTC]: the role of validation specialist shall be included as specified in BRG [5] and EVCG [4].*

No specific recommendations.

AUDIT LOGGING PROCEDURE

ETSI EN 319 411-1 states that

> *The requirements identified in ETSI EN 319 401 [8], clause 7.10 shall apply. In addition the following particular requirements apply:*
>
> *NOTE: See ETSI TS 101 533-1 [i.14] for provisions on how to preserve digital data objects.*
>
> *a) All security events shall be logged, including the security profile changes, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.*
>
> ***Registration***
>
> *b) All events relating to registration including requests for certificate re-key or renewal shall be logged.*
>
> *c) All registration information including the following shall be recorded:*
>
> *i) type of document(s) presented by the applicant to support registration;*
>
> *ii) record of unique identification data, numbers, or a combination thereof (e.g. applicant's driver's license number or code) of identification documents, if applicable;*

> *iii) storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 6.3.4, item d));*
>
> *iv) any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see clause 6.3.4, item d);*
>
> *v) identity of entity accepting the application;*
>
> *vi) method used to validate identification documents, if any; and*
>
> *vii) name of receiving TSP and/or submitting Registration Authority, if applicable.*
>
> *d) The TSP shall maintain the privacy of subject information.*
>
> ***Certificate generation***
>
> *e) The TSP shall log all events relating to the life-cycle of CA keys.*
>
> *f) The TSP shall log all events relating to the life-cycle of certificates.*
>
> *g) The TSP shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.*
>
> ***Revocation management***
>
> *h) The TSP shall log all requests and reports relating to revocation, as well as the resulting act*

Recommendations provided in 4.D related to log management apply to the perimeter described above.

RECORD ARCHIVAL

ETSI EN 319 411-1 states that

> *The following particular requirements apply:*
>
> *NOTE: See ETSI TS 101 533-1 [i.14] for provisions on how to preserve digital data objects.*
>
> *a) The TSP shall retain the following for at least seven years after any certificate based on these records ceases to be valid:*
>
> *i) log of all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA (see clause 6.4.5, item g));*
>
> *ii) Documentation as identified in clause 6.3.4.*

No specific recommendations.

COMPROMISE AND DISASTER RECOVERY

ETSI EN 319 411-1 states that

> *The requirements identified in ETSI EN 319 401 [8], clauses 7.9 and 7.11 shall apply. In addition the following particular requirements apply:*

Guidance provided in 4.D applies.

> ***TSP systems data backup and recovery***
>
> *a) TSP systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters.*
>
> *b) In line with ISO/IEC 27002 [i.7], clause 12.3: Back-up copies of essential information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.*

We propose the following recommendations regarding the term *regularly*

Security Level	**Proposed security measures**
Very high Security Level	Integrity of backup shall be checked after every backup. Complete recovery plan shall be tested every year.
High Security Level	Integrity of backup shall be checked at least on a week. Complete recovery plan shall be tested every 2 years.
Medium Security Level	Integrity of backup shall be checked at least on a month. Complete recovery plan shall be tested every 3 years.

> *c) Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.*

No specific recommendations.

> *d) [CONDITIONAL]: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.*

No specific recommendations.

> ***CA key compromise***
>
> *e) The TSP's business continuity plan (or disaster recovery plan) shall address the compromise or suspected compromise of a CA's private signing key as a disaster and the planned processes shall be in place.*

We recommend that such processes includes :

Communication plan
Revocation of certificates and destruction of private key
Collect of evidence for ferensics.

> *f) Following a disaster the TSP shall, where practical, take steps to avoid repetition of a disaster.*
>
> *NOTE: ISO/IEC 27002 [i.7] gives advice about the procedures to avoid it.*

No specific additional recommendation.

> ***Revocation status***
>
> *g) In the case of compromise the TSP shall as a minimum:*
>
> *i) inform the following of the compromise: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSPs. In addition, this information shall be made available to other relying parties;*

It is recommended to include these information in a communication plan.

> *ii) indicate that certificates and revocation status information issued using this CA key may no longer be valid; and*

No specific additional recommendation.

> *iii) revoke any CA certificate that has been issued for the compromised TSP when a TSP is informed of the compromise of another CA.*

No specific additional recommendation.

> ***Algorithm compromise***
>
> *h) Should any of the algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage then the TSP shall:*
>
> *i) inform all subscribers and relying parties with whom the TSP has agreement or other form of established*
>
> *relations. In addition, this information shall be made available to other relying parties; and*
>
> *ii) revoke any affected certificate.*

No specific additional recommendation.

CERTIFICATION AUTHORITY OR REGISTRATION AUTHORITY TERMINATION

B. CLAUSE 6.5 - TECHNICAL SECURITY CONTROLS

This clause, in addition of security requirements provided in ETSI EN 319 401 (see Section 4 of this document) specifies specific requirements covering the following area:

- Key pair generation and installation
- Private key protection and cryptographic module engineering controls
- Other aspects of key pair management such as certificate generation
- Activation Data
- Computer security controls
- Life cycle security controls
- Network security controls
- Timestamping

KEY PAIR GENERATION AND INSTALLATION

ETSI EN 319 411-1 states that

> *The requirements identified in ETSI EN 319 401 [8], clause 7.5 shall apply.*

See guidance provided in 4.D.

> *In addition the following particular requirements apply:*
>
> ***Certificate generation***
>
> *The CA shall generate subject keys securely and the subject's private key shall be secret.*
>
> *a) CA key generation and the subsequent certification of the public key, shall be undertaken in a physically secured environment (see clause 6.4.2) by personnel in trusted roles (see clause 6.4.4) under, at least, dual*
>
> *control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.*

For example, this can be done by generating the key in the operational environment or an equivalent (or with higher security) environment. Practices generally involve 3 to 10 people for such key ceremony. For example, the key generation may be handled by:

- Two operators under dual control
- A master of ceremony
- An independent witness.

> *b) CA key generation shall be performed using an algorithm recognized as being fit for the CA's signing purposes.*

> *NOTE 1: ETSI TS 119 312 [i.10] gives guidance on algorithms and their parameters.*

No specific additional recommendation.

> *c) The selected key length and algorithm for CA signing key shall be one which is recognized by industry as being fit for the CA's signing purposes.*
>
> *NOTE 2: ETSI TS 119 312 [i.10] gives guidance on algorithms and their parameters.*

No specific additional recommendation.

> *d) Before expiration of its CA signing key (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy.*

No specific additional recommendation.

> *e) These operations should be performed with a suitable interval between certificate expiry date and the last certificate signed to allow all parties that have relationships with the TSP (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a TSP which will cease its operations before its own certificate-signing certificate expiration date.*

It is recommended to setup a new certificate at least one year before the expiracy of the current one.

> *f) The TSP shall have a documented procedure for conducting key generation both on the root CA and subordinate, including CAs that issue certificates to end users. This procedure shall indicate, at least, the following:*
>
> *i) Roles participating in the ceremony (internal and external from the organization);*
>
> *ii) Functions to be performed by every role and in which phases;*
>
> *iii) Responsibilities during and after the ceremony; and*
>
> *iv) Requirements of evidence to be collected of the ceremony.*

It is specifically recommended to collect evidence of

- the date and place of the ley ceremony
- the algorithm used and the type and size of the keys

- the dual control of the operation
- a mean to identify the key in an non-ambiguous way (for example, by collecting a hash of the key)

We also recommend to write the key ceremony script in a way such that a non-specialist may understand and reproduce every step of the key ceremony.

> *g) The TSP shall produce a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. This report shall be signed:*
>
> *i) For root CA: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) and a trustworthy person independent of the TSP management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.*
>
> *ii) For subordinate CAs: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony as carried out.*
>
> *iii) [PTC]: clause 6.1.1.1 of the BRG [5] shall apply.*

We recommend that all participants of the key ceremony sign the report at the end of the ceremony.

> *Certificate generation and dissemination*
>
> *h) CA signature verification (public) keys shall be available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.*
>
> *NOTE 3: For example, CA public keys can be distributed in certificates signed by itself, along with a declaration that the key authenticates the CA, or issued by another CA. By itself a self-signed certificate cannot be known to come from the CA. Additional measures, such as checking the fingerprint of the certificate*
>
> *against information provided by a trusted source, is needed to give assurance of the correctness of this certificate.*

No specific additional recommendation.

> *Certificate generation / subject device provision*
>
> *[CONDITIONAL] If the CA generates the subject's keys:*
>
> *i) CA-generated subject keys shall be generated using an algorithm recognized by industry as being fit for the uses identified in the CP during the validity time of the certificate.*
>
> *j) CA-generated subject keys shall be of a key length and for use with a public key algorithm which are recognized by industry as being fit for the purposes stated in the CP during the validity time of the certificate.*
>
> *NOTE 4: ETSI TS 119 312 [i.10] gives guidance on algorithms and their parameters.*

> *k) CA-generated subject keys shall be generated and stored securely whilst held by the TSP.*

No specific additional recommendation.

> *Subject device provision*
>
> *l) The subject's private key shall be delivered to the subject's device or to the TSP managing the subject's private key, in a manner such that the secrecy and integrity of the key is not compromised. If the TSP or any of its designated RAs become aware that a subject's private key has been communicated to an unauthorized person or an organization not affiliated with the subject, then the TSP shall revoke all certificates that include the public key corresponding to the communicated private key:*
>
> *i) [PTC]: BRG [5], clause 6.1.24 shall apply.*

No specific additional recommendation.

> *m) Any copies of the subject's private key held by the TSP shall be destroyed after delivery of the private key to the subject.*

No specific additional recommendation.

> *n) [NCP+]: The TSP shall secure the issuance of a secure cryptographic device to the subject. In particular:*
>
> *i) Secure cryptographic device preparation shall be done securely.*
>
> *ii) Secure cryptographic device shall be securely stored and distributed.*

For example, security cryptographic device may be stored in a safe before and after each operation. Device proparation should be performed on dedicated workstation in secure premises.

PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Private key protection is widely discussed in a guidance regarding Article 24 and will not be further analysed in this guidance.

OTHER ASPECTS OF KEY PAIR MANAGEMENT SUCH AS CERTIFICATE GENERATION

> *The TSP shall use appropriately the CA private signing keys and shall not use them beyond the end of their life cycle*
>
> *In particular:*
>
> ***Certificate generation***

> *a) CA signing key(s) used for generating certificates, as defined in clause 6.3.3, and/or issuing revocation status information, shall not be used for any other purpose.*
>
> *b) The certificate signing keys shall only be used within physically secure premises.*
>
> *c) The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with current practice as in clause 6.5.1, item c).*
>
> *d) All copies of the CA private signing keys shall be destroyed or put beyond use at the end of their life cycle.*
>
> *e) [CONDITIONAL]: If a self-signed certificate is issued by the CA, the attributes of the certificate shall be compliant with the defined key usage as defined in Recommendation ITU-T X.509 [6] and aligned with point*

No specific additional recommendation.

ACTIVATION DATA

ETSI EN 319 411-1 states that

> *The following particular requirements apply:*
>
> ***Certificate generation***
>
> *a) The installation, activation and recovery of the CA's signing keys in a secure cryptographic device shall require simultaneous control of at least two trusted employees.*
>
> *NOTE 1: See also clause 6.5.1, item n).*

This requirement may be fulfilled by splitting the activation data between smartcard holders with a Shamir's Secret Sharing technics for example.

> ***Subject device provision***
>
> *[CONDITIONAL]: In particular, if the TSP issues a secure cryptographic device:*
>
> *b) Secure cryptographic device deactivation and reactivation shall be done securely.*
>
> *c) Where the secure cryptographic device has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure cryptographic device.*

In particular, TSP shall be very careful regarding the generation, storing, printing and deletion of the PIN code.

> *NOTE 2: Separation can be achieved by ensuring distribution of activation data and delivery of secure user device at different times, or via a different route.*

For example, the secure user device may be provided during a physical meeting and the PIN may be sent by registered mail.

COMPUTER SECURITY CONTROLS

ETSI EN 319 411-1 states that

> *The requirements identified in ETSI EN 319 401 [8], clause 7.4, items a) and f), shall apply.*

Guidance provided in 4.D applies.

> *NOTE: Requirements for the trustworthy systems can be ensured using, for example, systems conforming to CEN TS 419 261 [i.9] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [1].*
>
> *In addition the following particular requirements apply:*
>
> ***Certificate generation***
>
> *a) Local network components (e.g. routers) shall be kept in a physically and logically secure environment and their configurations shall be periodically checked for compliance with the requirements specified by the TSP.*

Security Level	Proposed security measures
Very high Security Level	**Configuration check may be done once a week**
High Security Level	**Configuration check may be done once a month**
Medium Security Level	**Configuration check may be done every three months**

> *b) The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.*

The following security measures may be adopted by TSP

Security Level	Proposed security measures
Very high Security Level	Authentication with qualified certificate
High Security Level	Authentication with qualified certificate
Medium Security Level	Authentication with certificate held on hardware token.

> ***Dissemination***
>
> *c) Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.*

TSP shall be specifically careful regarding data storing system such as databases.

> ***Certificate Revocation status***
>
> *d) Revocation status application shall enforce access control on attempts to modify revocation status information.*

TSP shall be specifically careful regarding :

- The protection of the CRL signing key. It is recommended to have the same security level that the certificate issuance signing key and adequate activation mechanism
- The system storig the revocation status information (e.g. Databases)

> ***Certificate generation and revocation management***
>
> *e) Continuous monitoring and alarm facilities shall be provided to enable the TSP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.*
>
> *EXAMPLE: This can use an intrusion detection system, access control monitoring and alarm facilities*

No specific additional recommendation.

LIFE CYCLE SECURITY CONTROLS

> *The requirements identified in ETSI EN 319 401 [8], clause 7.7 shall apply for all service components.*

See 4.D in this document for guidance regarding this point.

> *In addition the following particular requirements apply:*
>
> ***System planning***
>
> *a) [NCP]: capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available.*
>
> *b) [PTC]: clause 5 of the BRG [5] shall apply.*

No specific recommendations

> ***Certificate generation and revocation managemen***
>
> *c) See clause 6.5.5, item e).*

See Above.

NETWORK SECURITY CONTROLS

> *The requirements identified in ETSI EN 319 401 [8], clause 7.8 shall apply.*
>
> *In addition the following particular requirements apply:*
>
> *a) The TSP shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.*

No specific recommendations

> *b) The TSP shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.*

This may be done by disabling all elements by default and authorizing only he minimal needed for the operations.

> *c) The TSP shall grant access to secure zones and high security zones to only trusted roles.*

No specific recommendations.

> *d) The Root CA system shall be in a high security zone.*

It is recommended to operate root CAs offline.

TIMESTAMPING

> *NOTE: Not in the scope of the present document. See ETSI EN 319 421 [i.16] for policy requirements for TSPs issuing time-stamps.*

Not applicable

C. CLAUSE 7.1

This clause, in addition of security requirements provided in ETSI EN 319 401 (see Section 4 of this document) specifies specific requirements covering Certificate policy management.

> *The authority issuing a CP other than the ones defined in clause 5 shall demonstrate that the CP is effective.*
>
> *In particular, when the TSP issues other CPs:*

a) The CP shall identify which of the certificate policies defined in the present document it adopts as the basis, plus any variances it chooses to apply.

b) There shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the CP.

c) A risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the CP for the stated community and applicability.

d) CPs should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the CP.

e) A defined review process should exist to ensure that the CP is supported by the CA's CPS.

f) The TSP should make available the CPs supported by the TSP to its user community.

NOTE: The TSP's user community includes the subscribers/subjects eligible to hold certificates issued under the policy and any parties which may require relying upon those certificates.

g) Revisions to CPs supported by the TSP should be made available to subscribers and relying parties.

h) The CP shall incorporate, or further constrain, all the requirements identified in clauses 5 and 6 where they are

without a specific marking relating CP as specified in clause 5.

i) The CP shall specify the Recommendation ITU-T X.509 [6] certificate profile requirements.

j) [CONDITIONAL]: ETSI EN 319 412 part 2 to 4 [2], [9] and [10] should be used where appropriate.

k) A unique object identifier shall be obtained for the CP of the form required in Recommendation ITU-T X.509 [6].

No specific recommendations.

6. SPECIFIC MEASURES FOR TRUSTED SERVICES ISSUING QUALIFIED CERTIFICATES

The ETSI EN 319 411-2 provides a list of requirements for TSP issuing qualified certificates. In this document, specific security measures concerning certificate issuance services in the clauses 6.4, 6.5 and 7.1.

D. CLAUSE 6.4 - FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This clause cover the same areas that Clause 6.4 of ETSI EN 319 411-1. All requirements are the same except additional requirements concerning audit logging procedure stating that:

- TSP shall log all events relating to the preparation of QSCDs
- TSP shall set in place additional security measures concerning the logging of qualified certificate life-cycle.

E. CLAUSE 6.5 - TECHNICAL SECURITY CONTROLS

This clause cover the same areas that Clause 6.5 of ETSI EN 319 411-1. All requirements are the same except additional requirements concerning:

- The preparation of the QSSCD.
- The monitoring the QSSCD status

F. CLAUSE 7.1

This clause cover the same areas that Clause 7.1 of ETSI EN 319 411-1, but in addition, it is mentioned that all area described in Clause 5 and 6 of ETSI EN 319 411-2 shall be addressed (for example, that preparation of the QSSCD shall be addressed.

7. SPECTIFIC MEASURES FOR TRUSTED SERVICE ISSUING TIMESTAMPS

The standard ETSI TS 119 421/ EN 319 421 specifies security measures dedicated to time-stamping that may be set by TSP in addition to the ones of Section 4 of this document. These additional requirements concerns the TSA management and operation provided in Clause 7 and address specifically

- The Internal organization (Clause 7.2)
- The TSU Key Generation (Clause 7.6.2)
- TSU private key protection (Clause 7.6.3)
- TSU public key certification process (Clause 7.6.4)
- Rekeying process of TSU's key (Clause 7.6.5)
- Life cycle management of signing cryptographic hardware (Clause 7.6.6)
- End of TSU key life cycle (Clause 7.6.7)
- Time-stamp issuance (Clause 7.7.1)
- Clock synchronization with UTC (Clause 7.7.2)
- Physical and environmental security (Clause 7.8)
- Operation security (Clause 7.9)
- Network security (Clause 7.10)
- Collection of evidence (Clause 7.12)
- Business continuity management (Clause 7.13)
- TSA termination and termination plans (Clause 7.14)

8. SPECTIFIC MEASURES FOR SIGNATURE SERVICES

There is actually no published standard covering requirements for Signature services. The ongoing EN 119 101 is a European Norm based on ETSI technical specification TS 119 101. This specification may provide a list of requirements considered by industry as state of art of signature creation services and signature validation services.

9. SPECTIFIC MEASURES FOR VALIDATION SERVICES

There is actually no published standard covering requirements for Signature services. The ongoing EN 119 101 is a European Norm based on ETSI technical specification TS 119 101. This specification may provide a list of requirements considered by industry as state of art of signature creation services and signature validation services.

10. SPECTIFIC MEASURES FOR EDELIVERY SERVICES

There is actually no published standard covering requirements for eDelivery services. ETSI EN 319 511 (Policy and security requirements for registered electronic mail (REM) service providers) is planned to cover this scope.

11. SPECTIFIC MEASURES FOR SIGNATURE PRESERVATION SERVICES

There is actually no published standard covering requirements for preservation services. These requirements may be covered by these futures EN to be defined by ETSI.

- EN 319 521 Policy and security requirements for data preservation service providers
- EN 319 522 Data preservation services through signing
- EN 319 523 Conformity assessment of data preservation service providers