Telecommunications And Digital Government Regulatory Authority

TSP Framework

Guidelines for trust service practice statements

Issue date: 24/January/2024

Revision history

Version	Date	Description
1.0	24 January 2024	First version release

References

Reference	Title
[Law (3) 2003]	Federal Law by Decree No. 3 of 2003 Regarding the Organization of Telecommunications Sector
[Law (46) 2021]	Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services Version 20.09.2021 https://u.ae/en/about-the-uae/digital-uae/electronic-transactions-and-trust-services-law
[eIDAS]	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[EN 319 122-1]	ETSI EN 319 122-1 V1.3.1 (2023-06): Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: "Building blocks and CAdES baseline signatures"
[EN 319 122-2]	ETSI EN 319 122-2 V1.2.1 (2022-02) : Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: "Extended CAdES Signatures"
[EN 319 132-1]	ETSI EN 319 132-1 V1.2.1 (2022-02): Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
[EN 319 132-2]	ETSI EN 319 132-2 V1.1.1 (2016-04) : Electronic Signatures and Infrastructures (ESI); XAdES digital signatures ; Part 2 : Extended XAdES signatures
[EN 319 142-1]	ETSI EN 319 142-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
[EN 319 142-2]	ETSI EN 319 142-2 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles
[TS 119 182-1]	ETSI TS 119 182-1 V1.1.1 (2021-03): Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures
[EN 319 162-1]	ETSI TS 319 162-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); ASiC Associated Signature Containers; Part 1: Building blocks and ASiC baseline containers
[EN 319 102-1]	ETSI EN ETSI EN 319 102-1 V1.3.1(2021-11): Electronic Signatures and Infrastructures (ESI); Procedures for creation and validation of AdES Digital Signatures; Part1: Creation and Validation

[EN 319 411-1]	ETSI EN 319 411-1 v1.4.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[EN 319 411-2]	ETSI EN 319 411-2 v2.5.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[RFC 3647]	IETF RFC 3647(2003-11) : Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

Abbreviations

CA	Certification Authority
CPS	Certification Practice Statement
EU	European Union
ETSI	European Telecommunications Standards Institute
QTS	Qualified trust service
QTSP	Qualifier trust service provider
QTSP/QTSP	Qualified trust service provider and the qualified trust service(s) it provides
TDRA	Telecommunications And Digital Government Regulatory Authority
TSA	Time Stamping Authority
UAE	United Arab Emirates

Contents

1. Introduction

1.1. Context

In line with the objectives of the review of the existing UAE legislative framework, and with the following goals in particular:

- Setting a clear legal framework for electronic trust services in a national and cross-border context;
- Being prescriptive enough to increase the certainty of implementations meeting the provisions laid down by the legal framework and securing investments while paying attention in providing a welcoming environment for trust service providers and not creating unnecessary barriers;
- Having a clear, attractive but regulated framework for electronic trust services;

the objective of this document is to define implementation aspects, and among others, trust service practice statements templates. These templates can then be made prescriptive through references from the legislation, providing a clear and attractive technical framework for both trust service providers and relying parties.

In line with the following goal:

- Positioning the UAE amongst the international scene as meeting the highest level of international standards and best practices;

an additional objective of this document is to rely as much as possible on existing international standards, profiling them to the national context of UAE where applicable or necessary.

1.2. Scope of the present document

This present document is structured into two main sections:

Section 2 “Template for a Certification Practice Statement” specifies the template and guidelines for Certification Practice Statements (CPS) that can be used by (Qualified) Trust Service Providers (Q)TSP providing (qualified) certificates for electronic signatures and seals.

Section 3 “Template for a TSA Practice Statement” specifies the template and guidelines for TSA Practice Statements that can be used by QTSP providing qualified time-stamping services.

2. Template for a Certification Practice Statement

This section intends to provide a template and writing guidelines for (Q)TSP compliant with requirements specified in the UAE Trust Services Regulatory Framework **[Law (46) 2021] and [Bylaw (28) 2023]**, () as provider of the following trust service(s):

- Provision of certificates for website authentication;
- Provision of certificates for electronic signatures;
- Provision of certificates for electronic seals.
- Provision of qualified certificates for electronic signatures;
- Provision of qualified certificates for electronic seals.

As requirements specified for trust service providing (qualified) certificates for electronic signatures and seals are being based on requirements specified in ETSI [EN 319 411-1] and ETSI [EN 319 411-2], these standards may serve as further guidance for (Q)TSP in the writing of their CPS, as providing the general policy and security requirements that meet the requirements set out in the UAE Regulation.

The present template, with appropriate adjustment, may also serve as a baseline for other types of trust services.

CPS template structure

The template is structured in accordance with the Internet Engineering Task Force (IETF) [RFC 3647]. For the sake of readability, only the sections where further guidance is provided are hereinafter described. The proposed guidance is either on:

- The presence of subsections, further detailing the sections recommended by [RFC 3647]. These subsections translate common practices in CPS content.
- The content to be provided for the sections recommended by [RFC 3647]. This content may be specific to the UAE context. For general guidance regarding the content of all sections of the CPS, the (Q)TSP should refer to the [RFC 3647] itself.

2.1. Content of the template

1. Introduction

The following text shall be included:

This document constitutes _TSP/TS_ Certification Practice Statement (CPS) for the provision of _TYPES_OF_CERTIFICATES_. It is intended to describe the rules and procedures for the issuance and management of these types of certificates issued by _TSP/TS_, in particular regarding the registration of the subject, the generation of the certificate, the dissemination of relevant information (including the certificate itself), the potential revocation of the certificate, the publication of its revocation status, and (optionally) the provision of any related device to the subject.

This CPS complies with the formal requirements of IETF [RFC 3647] with regards to format and content. While certain section titles are included according to the structure of [RFC 3647], the topic may not necessarily apply in the specific implementation of the PKI services by the present TSP. Such sections only contain the text "Not applicable".

It is the responsibility of all parties applying for or using a digital certificate issued under this CPS, to read and understand this CPS and the related PKI Disclosure Statement (PDS).

1.1. Overview

The following text shall be included:

A (Q)TSPs providing, operating and/or selling (qualified) trust services in the UAE, is licensed by Telecommunications And Digital Regulatory Authority (TDRA), being the General Authority for Regulating the Telecommunications Sector, prior to starting the provision of operations. A candidate (Q)TSP aiming to provide (Q)TS in quality of (Q)TSP needs to be first granted a qualified status / a non-qualified status by the TDRA and this status included in the UAE trusted list, together with the identification of their respective trust services.

The licensing and respectively the grant of a qualified / non-qualified status to (Q)TSP/(Q)TS includes the requirement of an initial audit to be conducted when applying for the first time for a license (as well as for its renewal) to confirm that they meet the provisions of the UAE Regulation. This audit is further described in Section 8 of this present document.

This section shall explicitly list which Certificate Policy(ies) is(are) implemented by the present CPS, with their full names and object identifiers (OID), in particular for standardized CPs.

This section shall list the documents from the TSP this CPS refers to. For documents that are not publicly available in the repository, the CPS shall state how and if they can be made available (under a special agreement, or to specific authorized stakeholders such as auditors).

This section shall explicitly state which legal entity is ultimately liable for the present operations.

1.2. Document name and identification

The following text shall be included:

This document is the Certification Practice Statement (CPS) of _TSP_NAME_, and is recognized by the following identifications:

- *Title: _FULL_DOCUMENT_TITLE_*
- *Version: _DOCUMENT_VERSION_*
- *Object Identifier (OID): _CPS_OID_*

This CPS OID is inserted by reference within each Certificate Policy ruled by this CPS.

For the latest version of the present document, please refer to the repository at _REPOSITORY_URL_.

1.3. PKI Participants

Each type of participants shall be presented in a separate subsection.

1.3.1. Certification Authorities

The first subsection shall be “Certification Authorities”.

In addition to the recommendations of [RFC 3647], the CPS shall include in this subsection the complete CA hierarchy, including root and subordinate CA's. Each CA shall be unambiguously identified via its Subject Distinguish Name.

This hierarchy shall also clarify:

- The OID hierarchy of CP/CPS, separately or included in the same hierarchy where applicable.
- Where applicable, the existence of OCSP responders.

Regarding the rules applicable to the management of these OIDs, this section shall refer to section 9.12.

Other subsections shall be the following list, and in that order:

1.3.2. Registration Authorities

This subsection shall follow guidance from [RFC 3647] and clarify in particular:

- which RAs are under its responsibility along with the processes they manage;
- if any, which third party RAs or relevant entities are involved along with the processes they manage;
- how the interactions between the RA under the TSP's responsibility and the third party RAs or relevant entities are managed.

The TSP shall furthermore provide an organizational chart describing in details the relationships between all parties involved.

1.3.3. Subscribers

This subsection shall follow guidance from [RFC 3647] and clearly state the obligation of the subscribers, or refer to a document/section where they are stated.

1.3.4. Relying Parties

This section shall include the following content:

Obligations of relying parties are stated in section 4.5.2.

1.3.4. Other Participants

When there are no other participants, this section shall clearly state so.

1.4. Certificate usage

This section shall include the following content:

The limitations that apply to the usage of certificates issued under the present CPS are described in the following subsections.

This section shall contain two subsections:

1.4.1. Appropriate certificate usages

This subsection shall follow guidance from [RFC 3647] and/or refer to the CP(s).

1.4.2. Prohibited certificate usages

This subsection shall follow guidance from [RFC 3647] and/or refer to the CP(s).

1.5. Policy Administration

This section shall contain four subsections:

1.5.1. Organization administering the document

This organization is typically the TSP itself but shall be made explicit in the present section.

1.5.2. Contact Person

This subsection shall contain the precise contact information of the Policy Approval Authority related to the present CPS.

1.5.3. Person Determining CPS Suitability for the Policy

This subsection shall confirm that the Contact Person above is the Policy Approval Authority and as such determines the suitability and applicability of this CPS.

1.5.4. CPS Approval Procedures

This subsection shall contain a brief description of how the CPS is approved. This process shall involve the Policy Approval Authority listed above, and the repository has a means of public release of the CPS.

1.6. Definitions and Acronyms

Definitions and acronyms shall be compatible with Article 1 of [Law No.46/2021] together with abbreviations specific to the present document.

Reference documentation shall not be added here, but listed in annexure.

The two subsections shall be, separately:

1.6.1. Definitions

This subsection shall list all the definitions relevant to the present CPS.

1.6.2. Acronyms

This subsection shall list and explicit all the acronyms used in the present CPS.

2. Publication and Repository Responsibilities

If the CP(s) are separated from this CPS, these CP(s) shall be disclosed in the repository with a link to it. If the CP(s) are included in the present CPS, CPS-related information shall be clearly distinct from CP-related information.

2.1. Repositories

This section shall list the repositories used in relation with the present CPS. In particular, it shall clarify:

- The URL(s) of this(ese) repository(ies)
- The documents and information that shall be publicly available at these locations.

This list of documents shall include as a minimum:

- The CPS;
- The covered CPs, if separate from the CPS document;
- The related subscriber agreements (terms and conditions);
- The PKI Disclosure Statement (PDS);
- The CA certificates (the full chain from the root to the end-entity certificates);
- The test certificates;
- The CRLs;

2.2. Publication of Certification Information

This section shall clarify, where applicable:

- The URL(s) for downloading the CRL(s);
- The URL(s) of OCSP responder(s);
- If applicable, any other alternative regarding certificate validity status, such as a webpage;
- The URL(s) of the Certificates Public Registry.

2.3. Time or Frequency of Publication

This section shall specify as a minimum:

- The frequency at which CRLs are published.
- When applicable, the frequency at which delta CRLs are published.
- The maximum time after which approved versions of documents listed above are published in the repository(ies).

2.4. Access Controls on Repositories

This section shall confirm:

- what in the repositories is publicly-accessible with read-only rights (e.g. CPS, CP, OCSP responders, CRLs);
- what is of restricted access, if applicable;
- who is responsible for the publication of the information available in the repository(ies).
-

3. Identification and Authentication

3.1. Naming

3.1.1 Types of names

This subsection shall specify the standard(s) used for naming and the way they are implemented.

The TSP may add sections to the present subsection to that end.

3.1.2 Need for names to be meaningful

Following guidance from [RFC 3647], this subsection shall state whether the names have to be meaningful or not.

3.1.3 Anonymity and Pseudonymity of subscribers

This subsection shall clarify whether anonymity and pseudonymity is supported, and the way it is achieved when applicable.

3.1.4 Rules for interpreting various name forms

This subsection shall specify the way the types of names and their implementation is to be interpreted.

3.1.5 Uniqueness of names

This subsection shall clarify how the uniqueness of Subject Distinguished Name is ensured.

3.1.6 Recognition, authentication, and role of trademarks

This subsection shall specify as a minimum :

- whether the use of trademarks is allowed or not;
- the conditions under which it is permitted;
- the practices used to verify that the applicant is the rightful user of the trademark.

3.2. Initial Identity Validation

This section shall describe in details how compliance with every applicable requirement is achieved during the identification and authentication procedures for initial registration of the subscribers.

Depending on the type of certificate, this shall include in particular:

- How physical person identity validation is performed for certificates for electronic signatures;
- How legal entity identity validation is performed for certificates for electronic seals;

How domain validation is performed for web authentication certificates. Especially, in the case of provisions of qualified certificates, this section shall indicate whether the QTSP initially verifies the identity with:

- Physical presence of the person or their representative;
- Electronic Identification Tools, which provide an assurance of the actual presence of the person or their representative, and which meet the requirements of Article 21 of Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services on medium or high security levels;
- Qualified electronic signature or electronic seal authentication certificate;
- Any identification procedure applicable in the UAE which provides an equivalent confirmation of physical presence of the person, or of their representative, in terms of trust, provided that this equivalence is confirmed by the TDRA or its delegate, in terms of trust and security, and provided this confirmation is supported by audit from a Conformity Assessment Body that has conducted the audit in accordance with the provisions of this Law and of the regulations, standards, and decisions issued in implementation thereof.

As a minimum, this section shall contain four subsections:

3.2.1. Method to Prove possession of Private Key

If the key generation process by the subject or subscriber is allowed under the applicable policy, this subsection shall describe how the applicant is asked to demonstrate the possession of the private key.

If this process is not allowed or not applicable, it shall be made explicit.

3.2.2. Authentication of organization identity

This subsection shall describe how the validation of the identity of a legal person (e.g. the subject of a certificate for electronic seals) is performed.

3.2.3. Authentication of individual identity

This subsection shall describe how the validation of the identity of a natural person (e.g. the subject of a certificate for electronic signatures) is performed.

3.2.4. Non-verified subscriber information

This subsection shall detail which information is not subject to a verification by the TSP. Each non-verified information shall be clearly linked to specific type(s) of certificates, and refer to Section 7 for further details.

The subsection shall confirm that the subscriber is entirely responsible for providing accurate (and up-to-date) information during the registration process.

3.3. Identification and authentication for re-key requests

This section shall describe how identity is validated in the case of re-key requests. The process may differ depending on the type of re-key request.

3.3.1 Identification and authentication for routine re-key

This subsection describes a non-revoked non-expired certificate may be leveraged for a simplified re-key request (e.g. online request). This section may refer to Sections 4.7.

3.3.2 Identification and authentication for re-key after revocation

This section typically refers to Section 3.2 (or subsections of it) if the process is identical.

3.4 Identification and authentication for revocation requests

This subsection shall follow guidance from [RFC 3647] and clearly specify which individuals have the authority to request the revocation. This subsection shall in particular detail how the identification and validation of revocation requests may differ from the initial identity validation.

4 Certificate Life-Cycle Operational Requirements

Following guidance from [RFC 3647], separate consideration may need to be given to subordinate CAs, RAs, subscribers, and other participants.

4.1 Certificate Application

This section shall contain two subsections:

4.1.1 Who can submit a certificate application

This subsection identifies who can submit a certificate application, and in particular clarify which individuals are deemed legitimate to apply for a certificate for a Legal Entity.

4.1.2 Enrollment process and responsibilities

This subsection describes the enrollment process followed by the subscriber to submit a certificate application and the responsibilities pertaining to this process, and shall follow guidance from [RFC 3647].

4.2 Certificate Application Processing

This section describes the processing of certificate application and shall contain three subsections:

4.2.1 Performing identification and authentication functions

This subsection shall describe the identification and authentication procedures, keeping in mind that separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants.

4.2.2 Approval or rejection of certificate applications

This subsection shall describe the approval or rejection procedures of certificate applications, keeping in mind that separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants.

4.2.3 Time to process certificate applications

This subsection shall specify the time needed to process certificate applications, keeping in mind that separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants.

4.3. Certificate Issuance

In the case of provision of qualified certificates, this section shall contain as a minimum:

The issuance of certificates can only be done after obtaining a license (and, where applicable, a qualified status or a non-qualified status) from the TDRA in accordance with Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services. It is only when licensed and published in the UAE trusted list that the (Q)TSP is authorized to provide the corresponding licensed (Q)TS.

4.3.1 CA actions during certificate issuance

This subsection describes the actions taken by the CA during the issuance of the certificate and shall follow guidance from [RFC 3647].

This subsection typically refer to the CP(s).

4.3.2 Notification to subscriber by the CA of issuance of certificate

This subsection describes the practices followed by the CA to notify a subscriber of the issuance of the certificate it applied for and shall follow guidance from [RFC 3647].

4.4. Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

This subsection shall clarify:

- what are the actions a subscriber shall perform upon reception of the newly-generated certificate (e.g. test the certificate);
- when the certificate is deemed accepted (e.g. explicit / implicit acceptance).

This subsection shall clarify that the certificate shall be rejected in case of inaccuracy(ies).

4.4.2 Publication of the certificate by the CA

If there is no publication planned, this subsection shall state it clearly.

4.4.3 Notification of certificate issuance by the CA to other entities

If there is no notification to other entities planned, “Not applicable” shall be written under the title.

4.5. Key Pair and Certificate Usage

This section shall clarify that the use of the certificate and the corresponding private key is only permitted after agreement on the terms and conditions and acceptance of the certificate. The applicable terms and conditions shall be explicit from the certificate profile in Section 7, typically via the PDS.

Two subsections shall clarify separately duties for the subscriber and relying parties:

4.5.1. Subscriber private key and certificate usage

In the case of provisions of certificates for electronic signatures or certificates for electronic seals, this section shall contain as a minimum:

The subscriber commits to:

- *take the necessary care to avoid unauthorized use of the private key;*
- *notify the concerned persons immediately if the subscriber becomes aware that its private key used to create electronic signature/seal has been compromised, or if it finds from the surrounding circumstances that its used private key has been compromised;*
- *ensure the accuracy and completeness of its essential data in relation to the Qualified Certificate for the duration of its validity, in cases where such certification is required.*
- *report in the event of any changes to the information contained in the Qualified Certificate or if it is no longer confidential.*
- *a person whose Qualified Certificate has been suspended or revoked may not be reused by another Qualified TSP.*

4.5.2. Relying party public key and certificate usage

This subsection shall follow guidance from [RFC 3647] and state the responsibilities of parties relying on the subscriber’s public key and certificate.

4.6 Certificate renewal

This section shall follow guidance from [RFC 3647] and clearly state wether or not renewal is permitted.

A definition of ‘certificate renewal’ shall be included.

4.6.1 Circumstance for certificate renewal

This subsection shall follow guidance from [RFC 3647] and specify under which circumstances renewal is allowed.

4.6.2 Who may request renewal

This subsection shall follow guidance from [RFC 3647] and/or refer to the applicable CP(s).

4.6.3 Processing of certificate renewal requests

This subsection describes the practices followed by the CA when processing the requests for certificate renewal and shall follow guidance from [RFC 3647].

4.6.4 Notification of new certificate issuance to subscriber

This subsection describes the practices followed by the CA to notify a subscriber of the issuance of the new certificate and shall follow guidance from [RFC 3647].

4.6.5 Conduct constituting acceptance of a renewal certificate

This subsection shall follow guidance from [RFC 3647] and specify under which actions performed by the subscriber is the new certificate deemed accepted.

4.6.6 Publication of the renewal certificate by the CA

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

If there is no publication planned, this subsection shall state it clearly.

4.6.7 Notification of certificate issuance by the CA to other entities

This subsection shall follow guidance from [RFC 3647].

If there is no notification to other entities planned, this subsection shall state it clearly.

4.7 Certificate re-key

This section shall follow guidance from [RFC 3647] and clearly state wether or not re-keying is permitted.

A definition of 'certificate re-keying' shall be included.

4.7.1 Circumstances for certificate re-key

This subsection shall follow guidance from [RFC 3647] and specify under which circumstances re-keying is allowed.

4.7.2 Who may request certification of a new public key

This subsection shall follow guidance from [RFC 3647] and/or refer to the applicable CP(s).

4.7.3 Processing certificate re-keying requests

This subsection describes the practices followed by the CA when processing the requests for certificate re-key and shall follow guidance from [RFC 3647].

4.7.4 Notification of new certificate issuance to subscriber

This subsection describes the practices followed by the CA to notify a subscriber of the issuance of the new certificate and shall follow guidance from [RFC 3647].

4.7.5 Conduct constituting acceptance of a re-keyed certificate

This subsection shall follow guidance from [RFC 3647] and specify under which actions performed by the subscriber is the re-keyed certificate deemed accepted.

4.7.6 Publication of the re-keyed certificate by the CA

This subsection shall follow guidance from [RFC 3647].

If there is no publication planned, this subsection shall state it clearly.

4.7.7 Notification of certificate issuance by the CA to other entities

This subsection shall follow guidance from [RFC 3647].

If there is no notification to other entities planned, this subsection shall state it clearly.

4.8 Certificate modification

This section shall follow guidance from [RFC 3647] and clearly state wether or not modification is permitted.

A definition of 'certificate modification' shall be included.

4.8.1 Circumstances for certificate modification

This subsection shall follow guidance from [RFC 3647] and specify under which circumstances modification is allowed.

4.8.2 Who may request certificate modification

This subsection shall follow guidance from [RFC 3647] and/or refer to the applicable CP(s).

4.8.3 Processing certificate modification requests

This subsection describes the practices followed by the CA when processing the requests for certificate modification and shall follow guidance from [RFC 3647].

4.8.4 Notification of new certificate issuance to subscriber

This subsection describes the practices followed by the CA to notify a subscriber of the issuance of the modified certificate and shall follow guidance from [RFC 3647].

4.8.5 Conduct constituting acceptance of modified certificate

This subsection shall follow guidance from [RFC 3647] and specify under which actions performed by the subscriber is the modified certificate deemed accepted.

4.8.6 Publication of the modified certificate by the CA

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

If there is no publication planned, this subsection shall state it clearly.

4.8.7 Notification of certificate issuance by the CA to other entities

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

If there is no notification to other entities planned, this subsection shall state it clearly

4.9. Certificate Revocation and Suspension

This section shall clarify:

- How the revocation process is performed, in particular for validation of the request and publication of the revocation.
- How the synchronization between CRL and OCSP is performed, and its impact on relying parties.
- How and how long certificates are kept in CRL and OCSP responses after expiration.

In the case of provisions of qualified certificates, the section shall indicate that information regarding the validity or revocation of provided certificates is free of charge, automated, secure, available and efficient, at any time, including after the expiry of the certificate.

4.9.1 Circumstances for revocation

This subsection shall follow guidance from [RFC 3647] and explicit the circumstances under which a certificate must be revoked.

4.9.2 Who can request revocation

This subsection shall follow guidance from [RFC 3647] and/or refer to the applicable CP(s).

4.9.3 Procedure for revocation request

This subsection describes the procedure(s) used to request the revocation and shall follow guidance from [RFC 3647].

4.9.4 Revocation request grace period

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

4.9.5 Time within which CA must process the revocation request

This subsection shall follow guidance from [RFC 3647] and specify as a minimum:

- The time when the request will be processed, depending on the procedure used for the request (e.g. office hours for requests made by telephone);
- The maximum time frame allowed between receiving the request and performing it.

4.9.6 Revocation checking requirement for Relying Parties

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

4.9.7 CRL issuance frequency / OCSP response validity period

This subsection shall follow guidance from [RFC 3647] and specify as a minimum :

- The standards followed;
- how and how long certificates are kept in CRL and OCSP responses after expiration.

4.9.8 Maximum latency for CRLs

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

4.9.9 On-line revocation/status checking availability

This subsection shall follow guidance from [RFC 3647] and clearly show compliance with the standards used and the applicable law.

4.9.10 On-line revocation checking requirements

This subsection shall follow guidance from [RFC 3647] and clearly show compliance with the standards used and the applicable law.

4.9.11 Other forms of revocation advertisements available

This subsection shall follow guidance from [RFC 3647].

4.9.12 Special requirements regarding key compromise

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

4.9.13 Circumstances for suspension

This subsection shall follow guidance from [RFC 3647] and explicit the circumstances under which a certificate may be suspended.

4.9.14 Who can request suspension

This subsection shall follow guidance from [RFC 3647] and/or refer to the applicable CP(s).

4.9.15 Procedure for suspension request

This subsection describes the procedure(s) used to request the suspension and shall follow guidance from [RFC 3647].

4.9.16 Limits on suspension period

This subsection shall follow guidance from [RFC 3647].

4.10. Certificate Status Services

This section shall clarify:

- How CRLs and OCSP responders are made available.
- If these sources are directly identifiable and available from the information present in the certificate.
- How alternative methods are available, if applicable, and how these methods are machine-processable.
- Where applicable, any method and cost involved in the checking of a certificate revocation, including:
    - After the certificate has expired.
    - After the CA terminates or is compromised.
    - After the TSP terminates.

In the case of provisions of qualified certificates, the section shall indicate that information regarding the validity or revocation of provided certificates is free of charge, automated, secure, available and efficient, at any time, including after the expiry of the certificate.

4.10.1 Operational characteristics

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

4.10.2 Service availability

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

4.10.3 Optional features

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

4.11 End of Subscription

This section shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

4.12 Key Escrow and Recovery

This section shall follow guidance from [RFC 3647], clearly state whether or not key escrow and/or recovery features are provided, and provide further details about key storage when key escrow and/or recovery features are not provided.

4.12.1 Key escrow and recovery policy and practices

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable documentation.

4.12.2 Session key encapsulation and recovery policy and practices

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable documentation.

5 Facility, Management, and Operational Controls

This chapter shall follow guidance from [RFC 3647] and, when applicable, show compliance with the relevant standards.

5.1 Physical controls

This section shall follow the guidance from [RFC 3647] and clarify explicitly which physical controls are in place, in particular how the physical environment protects the certificate generation and revocation services.

5.1.1 Site location and construction

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.1.2 Physical access

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.1.3 Power and air conditioning

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.1.4 Water exposures

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.1.5 Fire prevention and protection

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.1.6 Media storage

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.1.7 Waste disposal

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.1.8 Off-site backup

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.2 Procedural controls

This section shall follow the guidance from [RFC 3647] and clarify explicitly which procedural controls are in place, in particular which key roles are identified, and how concepts such as segregation of duties and dual control are implemented.

5.2.1 Trusted roles

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.2.2 Number of persons required per task

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.2.3 Identification and authentication for each role

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.2.4 Roles requiring separation of duties

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.3.2 Background check procedures

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.3.3 Training requirements

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.3.4 Retraining frequency and requirements

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.3.5 Job rotation frequency and sequence

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.3.6 Sanctions for unauthorized actions

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.3.7 Independent contractor requirements

This subsection shall follow guidance from [RFC 3647]. and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

5.3.8 Documentation supplied to personnel

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.4. Audit logging procedures

This section shall follow guidance from RFC 3647 and clarify in particular:

- what types of events are recorded;
- how long these records are kept.

5.4.1 Types of events recorded

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

5.4.2 Frequency of processing log

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

5.4.3 Retention period for audit log

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

5.4.4 Protection of audit log

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.4.5 Audit log backup procedures

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.4.6 Audit collection system (internal vs. external)

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.4.7 Notification to event-causing subject

This subsection shall follow guidance from [RFC 3647] and clearly state whether it is applicable or not.

5.4.8 Vulnerability assessments

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.5. Records Archival

This section shall follow the guidance from RFC 3647 and clarify explicitly what is recorded, and how long it is kept. It shall clarify the availability and integrity of these records (in accordance with Law prescriptions).

5.5.1 Types of records archived

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.5.2 Retention period for archive

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.5.3 Protection of archive

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

5.5.4 Archive backup procedures

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

5.5.5 Requirements for time-stamping of records

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.5.6 Archive collection system (internal or external)

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

5.5.7 Procedure to obtain and verify archive information

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy.

5.6 Key changeover

This section shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

5.7. Compromise and Disaster Recovery

This section shall clarify which degraded level of service the TSP may offer to subscribers and to relying parties in case of disaster.

Among others, this section should cover topics such as:

- The CA arrangement in case of the CA key – compromise;
- The arrangement in case of end entity key compromise;
- The CA Incident Management plan;
- The CA Business Continuity / Disaster Recovery plan.

5.7.1 Incident and compromise handling procedures

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

5.7.2 Computing resources, software, and/or data are corrupted

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

5.7.3 Entity private key compromise procedures

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

5.7.4 Business continuity capabilities after a disaster

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

5.8. CA or RA Termination

This section shall clarify the termination activities, in particular the measures that have been taken regarding the obligations for records archival, last CRL, …

These termination activities shall be clear and regularly updated. This description shall not be “upon request”.

This description shall however not include any sensitive information.

6 Technical Security Controls

This chapter shall follow guidance from [RFC 3647] and, when applicable, show compliance with the relevant standards.

6.1 Key pair generation and installation

6.1.1 Key pair generation

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.1.2 Public key delivery to subscriber

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.1.3 Public key delivery to certificate issuer

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.1.4 CA public key delivery to relying parties

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.1.5 Key sizes

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.1.6 Public key parameters generation and quality checking

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2 Private key protection and cryptographic module engineering

6.2.1 Cryptographic module standards and controls

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.2 Private key (n out of m) multi-person control

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.3 Private key escrow

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.4 Private key backup

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.5 Private key archival

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.6 Private key transfer into or from a cryptographic module

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.7 Private key storage on cryptographic module

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.8 Method of activating private key

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.9 Method of deactivating private key

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.10 Method of destroying private key

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.2.11 Cryptographic module rating

This subsection shall follow guidance from [RFC 3647] and elaborate the corresponding practices that are used. If the subsection does not apply, “Not applicable” shall be the only content written after the title.

6.3 Other aspects of key pair management

6.3.1 Public key archival

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

6.3.2 Certificate operational periods and key pair usage periods

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

6.4 Activation data

6.4.1 Activation data generation and installation

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

6.4.2 Activation data protection

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

6.4.3 Other aspects of activation data

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

6.5.2 Computer security rating

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

6.6 Life cycle technical controls

6.6.1 System development controls

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

6.6.2 Security management controls

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

6.6.3 Life cycle security controls

This subsection shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

6.7 Network security controls

This section shall follow guidance from [RFC 3647] and state the corresponding practices that are used, referring to the applicable Certificate Security Policy

6.8. Timestamping

This section shall follow guidance from [RFC 3647] and describe in particular how the CA sources accurate time for activities such as certificate issuance or logging, certificate issuance.

7. Certificate and CRL Profiles

The following profiles shall be described in detail, either in the present document, or separately. If provided in a separate document, its reference shall be unambiguous (e.g. full name and version of a document, class of certificates to which it applies, …). The referenced document shall be publicly accessible from the repository.

The profiles shall clarify how test certificates can be identified unambiguously.

7.1. Certificate Profile

As a minimum, this section shall describe the certificate profiles of both the CA(s) issuing the end-entity certificates and the end-entity certificates. A certificate profile shall be provided for each type of these certificates. A certificate profile might be provided for higher level CAs in the hierarchy.

The description of the profile shall follow the below template:

Field	CE	O/M	CO	Value	Comment

The content of each column shall be as follows:

- Field: Shall contain the name of the field. Fields shall be grouped in categories corresponding to the ASN1 structure.
- CE: “Critical Extension”: T = True, F = False
- O/M: O = Optional, M = Mandatory

- Value:
    - For static values, this column shall specify the content (e.g. OID, URL, …).
    - For dynamic values, this column shall describe how the content is calculated and any template the value follows (e.g. format of an organization identifier based on a national register).
- Comment: Any additional comment regarding this field, particularly if the value is not validated by the TSP.

Each field of the profile shall be clearly specified. In particular for end-entity certificates, the profile shall specify how the following fields are managed / filled:

- Certificate
- Signature (algorithm and signatureValue)
- Version
- Issuer DN
- Subject DN
    - The profile shall clarify how the 'organisationIdentifier' attribute (2.5.4.97) is structured (e.g. usage of "VAT" or "NTR").
    - The profile shall clarify how the 'serialNumber ' is structured (e.g. usage of random number, or link to a national registry)
- Serial number
- Key size and underlying algorithms
- Certificate lifetime
- Authority Key Identifier
- Subject Key Identifier
- Basic Constraint
- Certificate Policies
- CRL Distribution Point
- Key Usage and Extended Key Usage
- Qualified Certificate Statements (as defined in ETSI EN 319 412-5)
- Authority Information Access
- Subject Alternative Name (e.g. RFC822 for email address of the subject, domain names for SSL/TLS certificates)

Where applicable, values of fields shall be presented with both their names and corresponding OIDs.

The profile shall specify how each certificate links to:

- The CPS;
- The applicable CP(s) / standardized CP(s).
- The applicable PKI Disclosure Statement (e.g. via the statement standardized in ETSI EN 319 412-5), identifying the applicable terms and conditions.

7.2. CRL Profile

The profile(s) shall follow the same template as the certificate profile above.

Each field of the profile shall be clearly specified. In particular, the profile shall specify how the following fields are managed / filled:

- Version
- Issuer DN
- nextUpdate (validity)
- revokedCertificates, reasonCode
- cRLNumber
- authorityKeyIdentifier
- ExpiredCertsOnCRL

7.3. OCSP Profile

The profile(s) shall follow the same template as the certificate profile above.

Each field of the profile shall be clearly specified. In particular, the profile shall specify how the following fields are managed / filled:

- Version
- Issuer DN
- Subject DN
- Serial number
- Key size and underlying algorithms
- Validity
- Authority Key Identifier
- Subject Key Identifier
- Basic Constraint
- Certificate Policies
- Key Usage and Extended Key Usage
- Authority Information Access
- OCSP No Revocation Checking (ocsp-nocheck)
- Subject Alternative Name

Where applicable, values of fields shall be presented with both their names and corresponding OIDs.

8. Compliance Audit and Other Assessment

This chapter shall refer to the TSP licensing scheme available on TDRA's website.

This section shall include a link to a publicly accessible website where the certificate of conformance may be found (e.g. website of the auditor, website of TDRA, …)

8.1. Frequency or circumstances of assessment

Based on the TSP licensing scheme referred above, this section shall focus on the licensing workflow.

In the case of the provision of qualified trust services, this section shall indicate that the QTSP is audited at least every 24 months by an independent Conformity Assessment Body.

8.2. Identity/Qualifications of Auditor

Based on the TSP licensing scheme referred above, this section shall focus on the accreditation scheme for Conformity Assessment Bodies. Especially, the name(s) of the Conformity Assessment Bodies should be clearly indicated, together with a link to their accreditation certificate.

8.3 Assessor's relationship to assessed entity

This section shall follow guidance from [RFC 3647].

8.4 Topics covered by assessment

This section shall follow guidance from [RFC 3647].

8.5 Actions taken as a result of a deficiency

This section shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

8.6 Communication of results

This section shall follow guidance from [RFC 3647] and state the corresponding practices that are used.

9 Other Business and Legal Matters

This chapter shall follow guidance from [RFC 3647].

9.1 Fees

9.1.1 Certificate issuance or renewal fees

This subsection shall follow guidance from [RFC 3647].

9.1.2 Certificate access fees

This subsection shall follow guidance from [RFC 3647].

9.1.3 Revocation or status information access fees

This subsection shall follow guidance from [RFC 3647].

9.1.4 Fees for other services

This subsection shall follow guidance from [RFC 3647].

9.1.5 Refund policy

This subsection shall follow guidance from [RFC 3647].

9.2. Financial Responsibility

In the case of the provision of qualified trust services, this section shall indicate that the QTSP is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations as a QTSP.

9.2.1 Insurance coverage

This subsection shall follow guidance from [RFC 3647].

9.2.2 Other assets

This subsection shall follow guidance from [RFC 3647].

9.2.3 Insurance of warranty coverage for end users

This subsection shall follow guidance from [RFC 3647].

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

This subsection shall follow guidance from [RFC 3647].

9.3.2 Information not within the scope of confidential information

This subsection shall follow guidance from [RFC 3647].

9.3.3 Responsibility to protect confidential information

This subsection shall follow guidance from [RFC 3647].

9.4. Privacy of Personal Information

This section shall confirm that personal data is processed in accordance with the provisions of local and federal data protection law.

9.4.1 Privacy plan

This subsection shall follow guidance from [RFC 3647].

9.4.2 Information treated as private

This subsection shall follow guidance from [RFC 3647].

9.4.3 Information not deemed private

This subsection shall follow guidance from [RFC 3647].

9.4.4 Responsibility to protect private information

This subsection shall follow guidance from [RFC 3647].

9.4.5 Notice and consent to use private information

This subsection shall follow guidance from [RFC 3647].

9.4.6 Disclosure pursuant to judicial or administrative process

This subsection shall follow guidance from [RFC 3647].

9.4.7 Other information disclosure circumstances

This subsection shall follow guidance from [RFC 3647].

9.5 Intellectual property rights

This section shall follow guidance from [RFC 3647].

9.6 Representation and warranties

This section shall follow guidance from [RFC 3647] and show compliance against ETSI EN 319 411-2 6.8.6**.**

9.6.1 CA representations and warranties

This subsection shall follow guidance from [RFC 3647].

9.6.2 RA representations and warranties

This subsection shall follow guidance from [RFC 3647].

9.6.3 Subscriber representations and warranties

This subsection shall follow guidance from [RFC 3647].

9.6.4 Relying party representations and warranties

This subsection shall follow guidance from [RFC 3647].

9.6.5 Representations and warranties of other participants

This subsection shall follow guidance from [RFC 3647].

9.7 Disclaimer of warranties

This section shall follow guidance from [RFC 3647].

9.8. Limitations of Liability

This section shall detail explicitly the limitations of liabilities of the TSP towards subscribers, subjects and relying parties.

9.9 Indemnities

This section shall follow guidance from [RFC 3647].

9.10 Term and termination

9.10.1 Term

This subsection shall follow guidance from [RFC 3647].

9.10.2 Termination

This subsection shall follow guidance from [RFC 3647].

9.10.3 Effect of termination and survival

This subsection shall follow guidance from [RFC 3647].

9.11 Individual notices and communications with participants

This section shall follow guidance from [RFC 3647].

9.12. Amendments

This section shall describe:

- How amendments are made to the present CPS, including the role of the Policy Approval Authority as described in Section 1.5;
- How the document version of the CPS is managed consequently to minor/major changes;
- Circumstances under which the CPS OID is changed consequently to minor/major changes, and how the document version and the OID are matched.

9.12.1 Procedure for amendment

This subsection shall follow guidance from [RFC 3647].

9.12.2 Notification mechanism and period

This subsection shall follow guidance from [RFC 3647].

9.12.3 Circumstances under which OID must be changed

This subsection shall follow guidance from [RFC 3647].

9.13 Dispute resolution provisions

This section shall be compliant with [EN 319 411-1] clause 6.8.13.

9.14. Governing law

This section shall follow guidance from [RFC 3647]. As a minimum, this section shall contain:

The services issued under this CPS are provided under the provisions of the Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services.

9.15. Compliance with Applicable Law

This section shall follow guidance from [RFC 3647]. If specific laws are applicable in addition to the ones mentioned in Section 9.14, the present section shall mention them.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This subsection shall follow guidance from [RFC 3647].

9.16.2 Assignment

This subsection shall follow guidance from [RFC 3647].

9.16.3 Severability

This subsection shall follow guidance from [RFC 3647].

9.16.4 Enforcement (attorneys' fees and waiver of rights)

This subsection shall follow guidance from [RFC 3647].

9.16.5 Force Majeure

This subsection shall follow guidance from [RFC 3647].

9.17 Other provisions

This section shall follow guidance from [RFC 3647].

ANNEXURE

A. References

This section shall list all the references used in this CPS. A first list is proposed below.

For standards (e.g. ETSI, CEN), references may either be specific (i.e. including the version number of the standard) or non-specific (i.e. not including the version number of the standard). In the latter case, the latest published version applies. For each of applicable references, the CPS shall explicit whether these are specific or non-specific references.

[Law No.46/2021]	Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services
[EN 319 401]	EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[EN 319 411-1]	EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[EN 319 411-2]	EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[EN 319 412-1]	EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[EN 319 412-2]	EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[EN 319 412-5]	EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[RFC 3647]	RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[TDRA SecLegQC]	TDRA Secondary legislation - Specific provisions for QTSP/QTS issuing QCs

3. Template for a TSA Practice Statement

This section intends to provide a template and writing guidelines for (Q)TSP compliant with requirements specified in the UAE Trust Services Regulatory Framework **[Law (46) 2021] and [Bylaw (28) 2023]**, as provider of (qualified) time-stamping services.

All subsequent references to [RFC 3647]* shall be understood as references to [RFC 3647] with appropriate changes so that it can apply to the context of time stamping, more precisely to a TSA Practice Statement. Those changes are quite straightforward and can include, not exclusively : no change at all, reading TSA in place of CA, disregarding mentions of certificate specific jargon such as CRL, replacing the content with adequate [RFC 3628] recommendations.
Furthermore, all subsequent references to [EN 319 421] shall be used with the amendments made in the applicable laws.

Structure of a TSA Practice Statement

ETSI [EN 319 421] specifies the policy and security requirements for (Q)TSP issuing time stamps, and is widely used among European QTSP providing this qualified trust service as a document structure to specify their TSA practice statement.

However, because [EN 319 421] is not a practice statement template as such, the following methodology has been proposed to design a TSA Practice Statement template:

- Observing that the structure for a CPS given by [RFC 3647] is holistic enough to cover every requirement laid down in [EN 319 411], therefore also covering the requirements laid down in [EN 319 401], we start with the same structure.
- Chapters and sections that are specific to the context of Certificate Authorities and cannot be adapted to the context of Time Stamping Authorities have to be removed.
- Time Stamping specific chapters and sections are added, following the structure of [EN 319 421] section 7.
- Finally, sections from [RFC 3647] that were not removed are adapted to the context of Time Stamping Authorities, either directly or following guidance from [RFC 3628].

Applying this methodology, Section 3.1 “Content of the template” proposes content guidelines that shall be considered together with the requirements laid down in [EN 319 421]. It is suggested to use these requirements as writing guidelines.

3.1. Content of the template

1. Introduction

The following text shall be included:

This document constitutes _TSP/TS_ Time Stamping Authority (TSA) Practice Statement for the provision of qualified time stamps. It is intended to describe the corresponding rules and procedures adopted by _TSP/TS_.

It is the responsibility of all parties applying for or using time stamps issued under this TSA Practice Statement, to read and understand this document and the related TSA Disclosure Statement.

1.1 Overview

The following text shall be included:

A (Q)TSPs providing, operating and/or selling (qualified) trust services in the UAE, is licensed by Telecommunications and Digital Regulatory Authority (TDRA), being the General Authority for Regulating the Telecommunications Sector, prior to starting the provision of operations. A candidate (Q)TSP aiming to provide (Q)TS in quality of (Q)TSP needs to be first granted a qualified status / a non-qualified status by the TDRA and this status included in the UAE trusted list, together with the identification of their respective trust services.

The licensing and respectively the grant of a qualified / non-qualified status to (Q)TSP/(Q)TS includes the requirement of an initial audit to be conducted when applying for the first time for a license (as well as for its renewal) to confirm that they meet the provisions of the UAE Regulation. This audit is further described in Section 7 of this present document.

This section shall explicitly list which TSA Policy(ies) is(are) implemented by the present TSA Practice Statement, with their full names and object identifiers (OID), in particular for standardized TSA Practice Statements.

This section shall list the documents from the TSP this TSA Practice Statement refers to. For documents that are not publicly available in the repository, this practice statement shall state how and if they can be made available (under a special agreement, or to specific authorized stakeholders such as auditors).

For documents that are publicly available, this practice statement shall indicate the location(s) of the online repository(ies) where they can be found.

This section shall explicitly state which legal entity is ultimately liable for the present operations.

1.2 Document name and identification

The following text shall be included:

This document is the TSA Practice Statement of _TSP_NAME_, and is recognized by the following identifications:

- *Title: _FULL_DOCUMENT_TITLE_*
- *Version: _DOCUMENT_VERSION_*
- *Object Identifier (OID): _TSA_PS_OID_*

[If the policy is a separate document] This TSA Practice Statement OID is inserted by reference within eachTSA Policy ruled by this TSA Practice Statement.

For the latest version of the present document, please refer to the repository at _REPOSITORY_URL_.

This section shall also list which TSA Policy(ies) is(are) implemented by the present TSA Practice Statement, with their full names and object identifiers (OID), in particular for standardized policies.

1.3 Time stamping services

This section shall contain a general presentation of the time stamping service and its purpose.

1.4 Participants

1.4.2 Time stamping authorities

In addition to the recommendations of ETSI [EN 319 421], this subsection includes the complete CA hierarchy, including root and subordinate CA's, down to the time stamping unit(s). Each CA shall be unambiguously identified via its Subject Distinguished Name (DN).

This hierarchy shall also clarify:

- The OID hierarchy of CP/CPS/TSA policy/TSA practice statement, separately or included in the same hierarchy where applicable.
- Where applicable, the existence of OCSP responders.

1.4.3 Subscribers

This subsection follows guidelines specified in clause 4.4 of [EN 319 421].

1.4.4. Relying Parties

This subsection shall identify and describe the relying parties and shall include the following text:

Relying parties are entities including natural or legal persons that rely on a time stamp token generated under this TSA Practice Statement. A Relying Party may or may not also be a Subscriber. The responsibility of the TSA towards the relying parties is limited in accordance with the provisions laid down in the Time-Stamp Policy.

Relying Parties are fully responsible for the decision of trusting or not a time stamp and thus has the obligation to identify and be aware of the conditions under which that time stamp has been issued.

1.4.5. Other Participants

If no other participants have been identified, "Not applicable" shall be the only content written under the title.

1.5. Policy Administration

This section shall contain four subsections:

1.5.1. Organization administering the document

This organization is typically the TSP itself but shall be made explicit in the present section.

1.5.2. Contact Person

This subsection shall contain the precise contact information of the Policy Approval Authority related to the present practice statement.

1.5.3. Person Determining TSA Practice Statement Suitability for the Policy

This subsection shall confirm that the Contact Person above is the Policy Approval Authority and as such determines the suitability and applicability of this TSA Practice Statement.

1.5.4. TSA Practice Statement Approval Procedures

This subsection shall contain a brief description of how the present practice statement is approved. This process shall involve the Policy Approval Authority listed above, and the repository has a means of public release of the practice statement.

1.6 Conformance

The following text is proposed:

The _TSP_NAME_ TSA references the policy identifier described in Section 5.2 "Identification" of this document in all time stamps to indicate conformance with this policy.

The _TSP_NAME_ TSA is subject to period independent internal and external reviews in order to demonstrate that _TSP_NAME_ TSA meets its obligations (cf. Section 6.5.1 "TSA Obligations") and has implemented appropriate controls as described in Section 7 "TSA Management and Operation".

1.7 Definitions and acronyms

Definitions and acronyms shall be compatible with Article 1 of [Law No.46/2021], [EN 319 421], and abbreviations specific to the present template.

1.7.1 Definitions

This subsection shall list all the definitions relevant to the present TSA PS.

1.7.2 Acronyms

This subsection shall list and explicit all the acronyms used in the present TSA PS

2. Publication and repository responsibilities

If the Time Stamping Policy(ies) are separated from this TSA PS, these Time Stamping Policy(ies) shall be disclosed in the repository with a link to it. If the Time Stamping Policy(ies) are included in the present TSA PS, TSA PS-related information shall be clearly distinct from Time Stamping Policy-related information.

2.1 Entity(ies) operating the repositories

This section shall confirm who is responsible for the publication of the information available in the repository(ies).

2.2 Repositories and Information published

This section shall list the repositories used in relation with the present TSA PS. In particular, it shall clarify:

- The URL(s) of this(ese) repository(ies)
- The documents and information that shall be publicly available at these locations.

This list of documents shall include as a minimum:

- The TSA PS;
- The covered TSA Policies, if separate from the TSA PS document;

- The related subscriber agreements (terms and conditions);
- The TSA Disclosure Statement.

This section shall aim to meet the requirement [EN 319 401] REQ-6.1-05A.

2.3 Time or frequency of publication

This subsection shall clarify the time and frequency of publication of the above mentioned information.

2.4 Access controls on repositories

This section shall confirm:

- what in the repositories is publicly-accessible with read-only rights (e.g. TSA PS, Time Stamping Policy);
- what is of restricted access, if applicable.

3. General Provisions

3.1 Obligations and Liability

This section shall include, directly or by reference, all the obligations, liabilities, guarantees, and responsibilities of the TSP, its Subscribers and Relying Parties

If by reference, this section shall clarify:

- How the applicable terms and conditions can be unambiguously identified from the content of a time stamp token;
- How these terms and conditions can be accessed (e.g. URL to the repository).

3.1.1 TSA obligations

This section focuses on the TSP obligations as specified in Section 6.5 of [EN 319 421].

3.1.2 Subscriber obligations

This section focuses on the Subscriber obligations as specified in Section 6.5.2 of [EN 319 421].

3.1.3. Relying parties' obligations

This section focuses on the Relying parties' obligations as specified in Section 6.6 of [EN 319 421].

3.1.4. Liability

This section focuses on the responsibility and liability of the TSP, and any limitation thereof.

In case of the provision of qualified time stamps, this section shall indicate that the QTSP is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations as a QTSP.

3.2 Time-stamp policy and TSA practice statement

As specified in clause 4.5 of [EN 319 421], this clause explains the relative roles of time-stamp policy and TSA practice statement. As [EN 319 421] places no restriction on the form of a time-stamp policy or practice statement specification, this section shall explicit if these are specified in the same or in different documents.

3.3 TSA disclosure statement

This section explicit how the TSA disclosure statement can be obtained:

- If this disclosure statement is contained in the present document, how and where it can be identified;
- If external to this document:
    - How the applicable disclosure statement can be unambiguously identified;
    - How it can be obtained (e.g. URL to the repository, reference to chapter 2).

3.4 Governing law

This section shall reference the governing law and follow guidance from [RFC 3647]* clause 4.9.14.

3.5 Compliance with applicable law

This section addresses the requirements REQ-7.13-01 and REQ-7.13-02 found in [EN 319 401] and shall follow guidance from both [RFC 3647]* clause 4.9.15 and [RFC 3628] clause 7.4.10 items b) and c).

4. Facility, management and operational controls

The chapter shall begin by addressing the requirements found in [EN 319 401] clauses 5, 6.3 and 7.3 before being subsequently divided in the following sections and subsections, following guidance from [RFC 3647]* clause 4.5:

4.1 Physical security controls

This section addresses the requirements found in [EN 319 421] clause 7.8. It shall follow the guidance from both [RFC 3647] clause 4.5.1 and [RFC 3628] clause 7.4.4 and clarify explicitly which physical controls are in place to protect the TSA's assets, in particular how compromise of the time stamping services is prevented.

4.2 Procedural controls

This section addresses the requirements REQ-7.4-04A to REQ-7.4-09 of [EN 319 401] in the below subsection. It shall follow the guidance from both [RFC 3647]* clause 4.5.2 and [RFC 3628] clause 7.4.3 items c) and f) to i), and clarify explicitly which procedural controls are in place, in particular which key roles are identified, and how concepts such as segregation of duties and dual control are implemented.

4.2.1 Trusted roles

This subsection shall follow guidance from [RFC 3647]* clause 4.5.2 and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.2.2 Number of persons required per task

This subsection shall follow guidance from [RFC 3647]* clause 4.5.2 and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.2.3 Identification and authentication for each role

This subsection shall follow guidance from [RFC 3647]* clause 4.5.2 and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.2.4 Roles requiring separation of duties

This subsection shall follow guidance from [RFC 3647]* clause 4.5.2 and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.3 Personnel controls

This section addresses the requirements found in [EN 319 421] clause 7.2 c) and 7.3 in the below subsections. It shall follow guidance from both [RFC 3647]* clause 4.5.3 and [RFC 3628] clause 7.4.3:

4.3.1 Qualifications, experience, and clearance requirements

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.3.2 Background check procedures

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.3.3 Training requirements

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.3.4 Retraining frequency and requirements

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.3.5 Job rotation frequency and sequence

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.3.6 Sanctions for unauthorized actions

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.3.7 Independent contractor requirements

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.3.8 Documentation supplied to personnel

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.4 Audit logging procedures

This section, in conjunction with the next section, addresses the requirements found in [EN 319 421] clause 7.12, which include the requirements found in [EN 319 401] clause 7.10, in the below subsections. It shall follow guidance from both [RFC 3647]* clause 4.5.4 and [RFC 3628] clause 7.4.11:

4.4.1 Types of events recorded

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used.

4.4.2 Frequency of processing log

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used.

4.4.3 Retention period for audit log

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used.

4.4.4 Protection of audit log

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.4.5 Audit log backup procedures

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.4.6 Audit collection system (internal vs. external)

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used.

4.4.7 Notification to event-causing subject

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used.

4.4.8 Vulnerability assessments

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.5 Records archival

This section, in conjunction with the previous section, addresses the requirements found in [EN 319 421] clause 7.12, which include the requirements found in [EN 319 401] clause 7.10, in the below subsections. It shall follow guidance from both [RFC 3647]* clause 4.5.5 and [RFC 3628] clause 7.4.11:

4.5.1 Types of records archived

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used.

4.5.2 Retention period for archive

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used.

4.5.3 Protection of archive

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.5.4 Archive backup procedures

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.5.5 Requirements for time stamping of records

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.5.6 Archive collection system (internal or external)

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used.

4.5.7 Procedure to obtain and verify archive information

This subsection shall follow guidance from [RFC 3647]* and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.6 Compromise and disaster recovery

This section addresses the requirements found in [EN 319 421] clause 7.11 and 7.13, in the below subsections. It shall follow guidance from both [RFC 3647]* clause 4.5.6 and [RFC 3628] clause 7.4.8.

4.6.1 Incident and compromise handling procedures

This subsection shall follow guidance from [RFC 3647]* and [RFC 3628], and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.6.2 Computing resources, software, and/or data are corrupted

This subsection shall follow guidance from [RFC 3647]*, and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.6.3 TSU's private key compromise procedures

This subsection shall follow guidance from [RFC 3647]* and [RFC 3628], and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.6.4 Loss of calibration of a TSU clock

This subsection shall follow guidance from [RFC 3628], and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.6.5 Business continuity capabilities after a disaster

This subsection shall follow guidance from [RFC 3647]* and [RFC 3628], and state the corresponding practices that are used, referring to the applicable TSA's Security Policy.

4.7 TSA termination and termination plans

This section addresses the requirements found in [EN 319 421] clause 7.14. It shall follow guidance from both [RFC 3647] clause 4.5.7 and [RFC 3628] clause 7.5.9, and clarify the termination activities.

These termination activities shall be clear and regularly updated. This description shall not be “upon request”.

This description shall however not include any sensitive information.

5. Time-stamping operational requirements

5.1 Time stamp request

This subsection shall specify the standards used for the time stamp request protocols, and how the TSA manages such requests.

5.2 Time stamp issuance

This subsection addresses the requirements found in [EN 319 421] clause 7.7.1 and shall specify the standards used for the time stamp response protocols, and how the TSA manages such response.

5.3 Clock synchronization with UTC

This subsection addresses the requirements found in [EN 319 421] clause 7.7.2.

5.4 Time stamp token profile

This subsection shall specify the standards used for the time stamp token profile, as well as the applicable laws.

5.5 Private key life cycle management

This subsection shall follow guidance from [RFC 3628] clause 7.2 and refer, when applicable, to sections 6.2 to 6.7.

5.6 TSU certificate revocation

This subsection clarify:

- Who can request a revocation
- The reasons of a revocation
- The procedures relating to the revocation

6. Technical security controls

6.1 Time accuracy

This subsection addresses the requirement found in [EN 319 421] clause 6.2 item b).

6.2 TSU key generation

This section addresses the requirements found in [EN 319 421] clause 7.6.2.

6.3 TSU private key protection

This section addresses the requirements found in [EN 319 421] clause 7.6.3.

6.4 TSU public key certificate

This section addresses the requirements found in [EN 319 421] clause 7.6.4.

6.5 Re-keying TSU's key

This section addresses the requirements found in [EN 319 421] clause 7.6.5.

6.6 Life cycle management of signing cryptographic hardware

This section addresses the requirements found in [EN 319 421] clause 7.6.6.

6.7 End of TSU key life cycle

This section addresses the requirements found in [EN 319 421] clause 7.6.7.

6.8 Computer security control

This section addresses the requirements REQ-7.8-16, REQ-7.8-17 and REQ-7.4-10 of [EN 319 401].

6.9 Life cycle security controls

This section addresses the requirements found in [EN 319 421] clause 7.9.

6.10 Network security controls

This section addresses the requirements found in [EN 319 421] clause 7.10

7. Compliance audit and other assessments

This section shall refer to the TSP licensing scheme available on TDRA's website.

This section shall include a link to a publicly accessible website where the certificate of conformance may be found (e.g. website of the auditor, website of TDRA, …)

As a minimum, the following sections shall be detailed in the TSA PS:

7.1 Frequency or circumstances of assessment

Based on the TSP licensing scheme referred above, this section shall focus on the licensing workflow.

This section shall indicate that the QTSP is audited at least every 24 months by an independent Conformity Assessment Body.

7.2 Identity/qualifications of assessor

Based on the TSP licensing scheme referred above, this section shall focus on the accreditation scheme for Conformity Assessment Bodies. Especially, the name(s) of the Conformity Assessment Bodies should be clearly indicated, together with a link to their accreditation certificate.

7.3 Assessor's relationship to assessed entity

This section shall follow guidance from [RFC 3647]* clause 4.8.

7.4 Topics covered by assessment

This section shall follow guidance from [RFC 3647]* clause 4.8.

7.5 Actions taken as a result of a deficiency

This section shall follow guidance from [RFC 3647]* clause 4.8.

7.6 Communication of result

This section shall follow guidance from [RFC 3647]* clause 4.8.

8. Other Business and Legal Matters

8.1 Fees

This section shall follow guidance from [RFC 3647]* clause 4.9.1.

8.1.1 Time Stamps issuance fees

This subsection shall follow guidance from [RFC 3647]*.

8.1.2 Fees for other services

This subsection shall follow guidance from [RFC 3647]*.

8.1.3 Refund policy

This subsection shall follow guidance from [RFC 3647]*.

8.2 Financial responsibility

This section shall indicate that the QTSP is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations as a QTSP.

This section addresses the requirement REQ-7.1.1-04 found in [EN 319 401], in the following subsections:

8.2.1 Insurance coverage

This subsection shall follow guidance from [RFC 3647]* clause 4.9.2.

8.2.2 Other assets

This subsection shall follow guidance from [RFC 3647]* clause 4.9.2.

8.2.3 Insurance of warranty coverage for end users

This subsection shall follow guidance from [RFC 3647]* clause 4.9.2.

8.3 Confidentiality of business information

This section shall follow guidance from [RFC 3647]* clause 4.9.3.

8.3.1 Scope of confidential information

This subsection shall follow guidance from [RFC 3647]*.

8.3.2 Information not within the scope of confidential information

This subsection shall follow guidance from [RFC 3647]*.

8.3.3 Responsibility to protect confidential information

This subsection shall follow guidance from [RFC 3647]*.

8.4 Privacy of personal information

This section shall indicate that personal data is processed in accordance with the provisions of local and federal data protection law.

This section addresses the requirement REQ-7.13-05 found in [EN 319 401], in the following subsections:

8.4.1 Privacy plan

This subsection shall follow guidance from [RFC 3647]* clause 4.9.4.

8.4.2 Information treated as private

This subsection shall follow guidance from [RFC 3647]* clause 4.9.4.

8.4.3 Information not deemed private

This subsection shall follow guidance from [RFC 3647]* clause 4.9.4.

8.4.4 Disclosure pursuant to judicial or administrative process

This subsection shall follow guidance from [RFC 3647]* clause 4.9.4.

8.4.5 Other information disclosure circumstances

This subsection shall follow guidance from [RFC 3647]* clause 4.9.4.

8.5 Intellectual property rights

This section shall follow guidance from [RFC 3647]* clause 4.9.5.

8.6 Representation and warranties

This section addresses the requirement REQ-6.3-05 and REQ-6.3-06 found in [EN 319 401], in the following subsections:

8.6.1 TSA representations and warranties

This subsection shall follow guidance from [RFC 3647]* clause 4.9.6.

8.6.2 Subscriber representations and warranties

This subsection shall follow guidance from [RFC 3647]* clause 4.9.6.

8.6.3 Relying party representations and warranties

This subsection shall follow guidance from [RFC 3647]* clause 4.9.6.

8.6.4 Representations and warranties of other participants

This subsection shall follow guidance from [RFC 3647]* clause 4.9.6.

8.7 Disclaimer of warranties

This section shall follow guidance from [RFC 3647]* clause 4.9.7.

8.8 Limitations on liability

Limitations on liability are covered in the terms and conditions as per clause 9.4. (Excerpt from ETSI)

8.9 Indemnities

This section shall follow guidance from [RFC 3647]* clause 4.9.9.

8.10 Term and termination

This section addresses the requirement REQ-6.1-10 found in [EN 319 401], in the following subsections:

8.10.1 Term

This subsection shall follow guidance from [RFC 3647]* clause 4.9.10.

8.10.2 Termination

This subsection shall follow guidance from [RFC 3647]* clause 4.9.10.

8.10.3 Effect of termination and survival

This subsection shall follow guidance from [RFC 3647]* clause 4.9.10.

8.11 Individual notices and communications with participants

This section shall follow guidance from [RFC 3647]* clause 4.9.11.

8.12 Amendments

This section shall describe:

- How amendments are made to the present CPS, including the role of the Policy Approval Authority as described in Section 1.5;
- How the document version of the CPS is managed consequently to minor/major changes;
- Circumstances under which the CPS OID is changed consequently to minor/major changes, and how the document version and the OID are matched.

This section shall explicit which of these OIDs are referenced in the issued time stamp tokens.

8.12.1 Procedure for amendment

This section addresses the requirement REQ-6.1-08 found in [EN 319 401].

8.12.2 Notification mechanism and period

This section addresses the requirement REQ-6.1-09A found in [EN 319 401].

8.12.3 Circumstances under which OID must be changed

This subsection shall follow guidance from [RFC 3647]*.

8.13 Dispute resolution provisions

This section addresses the requirements REQ-6.2-02 item h) and REQ-7.1.1-06 found in [EN 319 401].

8.14 Miscellaneous provisions

This section shall follow guidance from [RFC 3647]* clause 4.9.16.

8.14.1 Entire agreement

This subsection shall follow guidance from [RFC 3647]*.

8.14.2 Assignment

This subsection shall follow guidance from [RFC 3647]*.

8.14.3 Severability

This subsection shall follow guidance from [RFC 3647]*.

8.14.4 Enforcement (attorneys' fees and waiver of rights)

This subsection shall follow guidance from [RFC 3647]*.

8.14.5 Force Majeure

This subsection shall follow guidance from [RFC 3647]*.

8.15 Other provisions

This chapter shall follow guidance from [RFC 3647]* clause 9.17.

8.15.1 Organizational

This section addresses the requirements found in [EN 319 421] clause 7.2.

8.15.2 Additional testing

This section shall follow guidance from [RFC 3647]* clause 9.17.

8.15.3 Disabilities

This section addresses the requirements REQ-7.13-03 and REQ-7.13-04 found in [EN 319 401].

8.15.4 Terms and conditions

This section addresses the requirements found in [EN 319 421] clause 6.3.

ANNEXURE

A. References

This section shall list all the references used in this TSA Practices Statement. A first list is proposed below.

For standards (e.g. ETSI, CEN), references may either be specific (i.e. including the version number of the standard) or non-specific (i.e. not including the version number of the standard). In the latter case, the latest published version applies. For each of applicable references, the TSA Practices Statement shall explicit whether these are specific or non-specific references.

[Law No.46/2021]	Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services
[EN 319 401]	EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[EN 319 421]	EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[EN 319 422]	EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[RFC 3628]	RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs)