ZETES TSP QUALIFIED CA 001

E-SEAL CERTIFICATE POLICY FOR SELF-MANAGED (Q)SCD

NCP+, QCP-l, and QCP-l-qscd

Publication date :	**10/03/2023**	
Effective date :	**12/03/2023**	
CP OID :	**1.3.6.1.4.1.47718.2.32.2021.1.3.20.1112.3.2 1.3.6.1.4.1.47718.2.32.2022.1.6.21.1112.3.2 1.3.6.1.4.1.47718.2.32.2022.1.7.20.1112.3.2**	
Version :	**1.2**	**06/03/2023**

Table of Content

Tables

ABOUT THIS DOCUMENT

Scope

The present document is the Certificate Policy (CP) document for Zetes TSP Qualified CA 001 for the issuance of certificates issued to legal persons.

Issued certificates meet the requirements of Regulation (EU) No 910/2014 **[ref. 1]** and the requirements for Trust Service Providers issuing

- [NCP+] certificates under ETSI EN 319 411-1 **[ref. 2]** or
- [QCP-l] & [QCP-l-qscd] EU Qualified certificates under ETSI EN 319 411-2 **[ref. 3]**.

Intellectual Property Rights

Without limiting the "all rights reserved" copyright on the present document, and except as duly licensed under written form, no part of this document or any of its contents may be reproduced, copied, modified or adapted, without the prior written consent of the author, unless otherwise indicated for stand-alone materials.

Commercial use and distribution of the contents of this document is not allowed without express and prior written consent of Zetes SA.

The following sentence must appear on any copy of this document:

"© 2017 – Zetes – All Rights Reserved"

DOCUMENT VERSION HISTORY

Version	Publication Date	Effective Date	Information about this Version
1.2	09/03/2023	11/03/2023	Addition of QCP-l offering.
1.1	07/03/2022	09/03/2022	Corrections in OID for QCP-l-qscd offering.
1.0	06/07/2021	07/07/2021	First publication ---

REFERENCES

[ref. 1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[ref. 2] ETSI EN 319 411-1: “Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements”

[ref. 3] ETSI EN 319 411-2: “Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates”

[ref. 4] ZETESCONFIDENS Trust Services Practice Statement (TSPS) (ZETESCONFIDENS document OID 1.3.6.1.4.1.47718.2.0.1.1)

[ref. 5] ZETESCONFIDENS Certificate Practice Statement (CPS) for Zetes TSP Qualified CA 001 (ZETESCONFIDENS document OID 1.3.6.1.4.1.47718.2.1.1.2)

[ref. 6] ZETESCONFIDENS Certificate Terms and Conditions (CTC)

1. INTRODUCTION

1.1 Overview

Conformity with European legislation and standards for Trust Service Providers issuing certificates

ZETESCONFIDENS is a Qualified Trust Service Provider in the sense of the Regulation (EU) No 910/2014 **[ref. 1]**. To this regard, ZETESCONFIDENS is supervised by the Belgian Federal Public Service Economy, SMEs, the Self-Employed and Energy - Quality and Safety, the Belgian Supervisory Body for the provisioning of trust services.

ZETESCONFIDENS is the Trust Service Provider (TSP) and has final and overall responsibility for the provision of the ZETESCONFIDENS certificates offering for Certificates issued to legal persons, namely:

- Registration service through the ZETESCONFIDENS Registration Authority: verifies the full name of the organizational entity and the registration information of the legal person including a nationally recognized identifier and if applicable, any specific attributes of the subject. The results of this service are passed to the certificate generation service.
- Certificate generation service through the ZETESCONFIDENS Certification Authority (CA): creates and signs certificates based on the identifiers and attributes verified by the registration service.
- Key generation witnessing (where applicable) for keys generated on infrastructure not operated by ZETESCONFIDENS.
- Dissemination service for certificates, public terms and conditions, policy and practice information, to subscribers and relying parties.
- Revocation management service through the ZETESCONFIDENS Suspension and Revocation Authority: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the certificate status service.
- Certificate status information service: provides certificate revocation status information to relying parties.

CP related documents governing the provision and use of certificates issued to legal persons

For practices regarding the issuing of Certificates to legal persons, reference is made to the common trust service provisioning practices non-specific to the issuance of such certificates, provided in the TSPS [ref. 4], and the applicable CPS [ref. 5].

The end entity certificates issued by this CA contain the ZETESCONFIDENS proprietary Certificate Policy OID as well as the relevant ETSI Certificate Policy OID corresponding to the type and the assurance level of the Certificate:

Certificate Policy	Policy Description
ETSI QCP-l 0.4.0.194112.1.1	Certificate policy for European Union (EU) qualified certificates (conforming to ETSI EN 319-411-2) issued to legal persons.
ETSI QCP-l-qscd 0.4.0.194112.1.3	Certificate policy for European Union (EU) qualified certificates (conforming to ETSI EN 319-411-2) issued to legal persons with private key related to the certified public key in a Qualified electronic Signature/seal Creation Device (QSCD).
ETSI NCP+ 0.4.0.2042.1.2	NCP+ (Normalized Certificate Policy requiring a secure user device) certificate policy.

Non-disclosure

For reasons of confidentiality, ZETES cannot disclose all details on controls in this document, but instead included references to internal detailed documents. These documents will only be made available to duly authorised parties. Section 3.6 of the RFC 3647 and clause 5.2 of the ETSI EN 319 411-1 allow for the use of references to distinguish disclosures between public information and security sensitive confidential information.

1.2 Document name and identification

Document name:

Zetes TSP Qualified CA 001

e-Seal Certificate Policy for self-managed (Q)SCD

Policy document OID:

Certificate policy	ETSI Certificate Policy OID	ZETESCONFIDENS Certificate Policy OID
ETSI QCP-l	0.4.0.194112.1.1	1.3.6.1.4.1.47718.2.32.2022.1.7.20.1112.3.2
ETSI QCP-l-qscd	0.4.0.194112.1.3	1.3.6.1.4.1.47718.2.32.2022.1.6.21.1112.3.2
ETSI NCP+	0.4.0.2042.1.2	1.3.6.1.4.1.47718.2.32.2021.1.3.20.1112.3.2

Proprietary Certificate Policy OIDs:

ETSI policy	Proprietary CP OID	Description
NCP+ 0.4.0.2042.1.2	1.3.6.1.4.1.47718.2.32.2021.1.3.20.1112.3.2	(NCP+ type) certificate on self-managed SCD for advanced electronic seal
QCP-l 0.4.0.194112.1.1	1.3.6.1.4.1.47718.2.32.2022.1.7.20.1112.3.2	(QCP-l type) certificate on non-qualified SCD (self-managed by a third party, subscriber or subject)
QCP-l-qscd 0.4.0.194112.1.3	1.3.6.1.4.1.47718.2.32.2022.1.6.21.1112.3.2	(QCP-l type) certificate on self-managed QSCD for qualified electronic seal

1.3 PKI participants

1.3.1 Subscribers and Subjects

In the case of certificates issued for electronic seals, the Subject is either the legal person itself or an organizational entity (department, unit, government entity, business entity or non-commercial entity) identified in association with the legal person.

The Subscriber, requesting a certificate for a legal person, is any entity as allowed under the relevant legal system to represent the legal person, subscribing for that legal person or its units or departments (the Subject).

Therefore, Subscribers are an entity (managing director, board of director, head of administration, …) representing the legal person (private company, government, institution, …) identified by the Subject.

The Subscriber, as a legal representative of the legal person, acts on behalf of the latter. As such any action of the Subscriber shall be attributed to the legal person and any information provided to the Subscriber shall be considered to be provided also to the Subject.

1.3.2 Other PKI participants

Information can be found in the CPS [ref. 5].

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The certificates issued under this policy are intended for the creation of electronic seals on behalf of the Subject.

The certificate usage is encoded in the certificate itself by means of the keyUsage and policyIdentifier fields in compliance with the following relevant standards:

- ETSI EN 319 411-1
- ETSI EN 319 411-2
- ETSI EN 319 412-1
- ETSI EN 319 412-3
- ETSI EN 319 412-5
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile

It is the responsibility of the Subject to use certificates only according to the intended usage and restrictions of the present policy.

For validation of the electronic seal based upon a certificate issued under the present policy it is the responsibility of the Relying Party to use means that correctly interpret, display and use the information and usage restrictions encoded in the certificates, such as but not limited to key usage, limited liability per transaction, certificate validity, etc.

It is the responsibility of the Subject and the Relying Party to decide for which purpose the certificates are considered trustworthy. A Relying Party must always take into account the level of assurance and other information in the CPS and CP before deciding on the applicability or the acceptance of the certificate.

1.4.2 Prohibited certificate uses

Any usage of a certificate other than the usage explicitly allowed in the present CP is prohibited.

1.5 Policy administration

Information can be found in the CPS [ref. 5].

1.6 Definitions and acronyms

1.6.1 Acronyms

See **[ref. 5]**.

1.6.2 Definitions

See **[ref. 5]**.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ZETESCONFIDENS operates services 24/7 for the publication of information as described in [ref. 4.]

The CA certificate and certificate status information is made available in formats and through protocols that support automated certificate validation by standard-compliant software applications.

Where applicable the information is also available for manual download from the ZETESCONFIDENS web site. Public statements and other public information such as the Certification Practice Statement documents, Certificate Policy documents, etc. are available for download from the same web site.

The URLs for the online repositories and certificate download services specific to this CA are repository.confidens.zetes.com and crt.confidens.zetes.com. The URLs for the certificate status services are listed in the certificate profile information in section 7.

2.2 Publication of certification information

Availability

See [ref. 4].

Publication of Subject certificates in a repository

Under this policy certificates issued to Subjects (end entity certificates) are not published in a public certificate repository.

The CA does not issue end entity certificates for encryption, therefore a third party has no need to retrieve a Subject's certificate from a central repository,

The Subject is expected to use protocols and formats for electronic seals that include the certificates with the signed data and thereby enable the Relying Party to retrieve the certificates from the sealed object.

It is the responsibility of the Relying Party to extract the certificate chain from the signed object and validate the entire chain of the extracted certificate correctly.

Publication of CA certificates in a repository

The CA certificates are published in a public certificate repository (http://crt.confidens.zetes.com). The CA certificates can be downloaded manually by or automatically by software applications. The fingerprint information for these certificates is stated in section 7.

Relying parties who wish to validate these values before installing the CA certificates can request out-of-band confirmation via info@confidens.zetes.com.

Certificate Status Information

See section 4.10.

2.3 Time or frequency of publication

Publication of CA certificates in a repository

CA Certificates are published in the repository before end-entity certificates emanating from these CAs are made available to the Subjects.

Certificate Status Information

See section 4.10.

Dissemination of public information

Updates to this document or other public documents are published whenever a change occurs. Under normal conditions a period of minimum two (2) days will be observed between the publication date and the effective date.

2.4 Access controls on repositories

Only authorized staff and internal systems of ZETESCONFIDENS have access rights to update, delete or create new resources in these repositories.

Public documents are available for download to all interested parties via the repositories (see section 2.1).

ZETESCONFIDENS will take reasonable measures to protect and prevent against abuse of the repositories and the OCSP service and will strive to give all parties equal and unhindered access.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

For the purpose of conforming to ETSI EN 319 411-1 **[ref. 2]** and to the requirements stated in the Regulation (EU) No 910/2014 **[ref. 1]**, the name attributes in the end entity certificates for legal persons are compliant with the ETSI EN 319 412 part 1 and part 3, and Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015.

Many software applications use the **commonName** when showing a certificate to the end user. For this reason, the **commonName** field may also incorporate plain wording describing the intended usage or context of the certificate.

3.1.2 Need for names to be meaningful

Certificate Attribute	Description
organizationName	**Official registered name of the Subject as a corporation or organization** It is representing the full registered name of the organizational entity (private organization, government entity, business entity or non-commercial entity) consistent with the national or other applicable identification practices.
organizationIdentifier	**Official registered unique number or unique identifier of the Subject as a corporation or organization** formatted as specified in ETSI EN 319 412-1 optionally together with a semantic identifier. It is representing the registration number of the organization as stated in the official records.
commonName	**Official name or calling name of the Subject + optional indication of the intended purpose or context for this certificate** The certificate will only contain one instance of commonName. The commonName is intended for a user friendly representation of the Subject name and the certificate's purpose or context.
countryName	**Country where the organisation is established**.
organizationUnitName	**OPTIONAL Name of a department, division or system.**
Locality	**OPTIONAL City or municipality in which the Subject is incorporated.**

3.1.3 Anonymity or pseudonymity of Subjects

The CA does not issue certificates that use pseudonyms or any form of anonymous identifiers.

3.1.4 Rules for interpreting various name forms

The names used in the certificates are for legal persons. See section 3.1.1 and section 3.1.2.

3.1.5 Uniqueness of names

A Subject may have more than one certificate with the same DN. The DN is guaranteed to be unique for the Subject by virtue of the unique organizationIdentifier.

3.1.6 Recognition, authentication, and role of trademarks

No stipulations.

3.2 Initial identity validation

Initial identity validation is performed as the registration process or onboarding process for a Subject by the RA.

3.2.1 Method to prove possession of private key

Private Key generated by the Subject/Subscriber

The Subscriber must submit a Certificate Signing Request (CSR) which contains the public key and which must be signed with the corresponding private key. The CSR file will be stored as evidence to proof possession by the Subject.

3.2.2 Authentication of organization identity

The Subject's identity is authenticated in accordance with the rules and regulations for the naming and identification of organizations as applicable in the country where the legal person is established. The Subject is the same as the legal person or is an integral organizational unit of the legal person.

3.2.3 Authentication of individual identity

The signed Registration Form confirms:

- Full identification details of the Subject and Subscriber
- (where applicable) Full identification details and contact information of the authorised natural person representing the Subscriber
- Full identification details and contact information of the Certificate Manager. The Certificate Manager is the single point of contact for the CA for the exchange of certificate creation requests and certificate revocation requests.
- Acceptance of the Subscriber Agreement with Terms & Conditions
- Exhaustive list of the certificate(s) being requested including the DN, certificate policy OID and certificate validity period.

The registration form is electronically signed by (the representative of) the Subscriber and by the Certificate Manager with qualified electronic signatures.

3.2.4 Validation of authority

The representative's authorization to represent the Subject Subscriber is verified against the nationally recognised register(s) that identify the Subscriber and its authorized representatives or against the Subscriber's articles of incorporation.

3.2.5 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Routine re-key requests are processed as new certificate requests.

3.3.2 Identification and authentication for re-key after revocation

Re-key requests after revocation are processed as new certificate requests.

3.4 Identification and authentication for revocation request

The CA has the right to revoke certificates as it sees fit. Revocation by the CA follows procedures that are internal to the CA. The Subscriber can submit revocation requests via e-mail by means of an electronically signed revocation form or through an authenticated channel. For the revocation request procedure, see Section 4.1 of the TSPS.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Only the legally authorized representative of the Subscriber can request a certificate on behalf of the Subscriber. The Subscriber must comply with the provisions and obligations set forth in the registration form (see section 3.2.3), in the applicable Subscriber Agreement, in this CP and in the Terms and Conditions.

4.1.2 Enrolment process and responsibilities

4.1.2.1 Responsibilities of the RA in the Enrolment Process

The enrolment process is handled by the ZETESCONFIDENS Registration Authority .

The RA verifies:

- the claimed identity of the applicant and of the applicant's representative(s),
- the authorization of the representative,
- (when applicable) the proof of possession of the private key,
- (when applicable) the (Q)SCD compliance of the Subject's Seal Creation Device.

This enrolment process is done in accordance with the rules and methods described in this document and in internal guidelines and rules. The RA archives the received or added information for each certificate request.

4.1.2.2 The Subject Enrolment Process

The RA collects the required documents and attestations in the application process for the subsequent validation of the applicant's identities and authorisations and the CSR.

The application starts with the signed registration form (see Section 3.2.3).

Identity of the Subject is verified according to Section 3.2.2.

Identity of the authorized representative and its authorization to commit the Subject is verified according to Section 3.2.3 and Section 3.2.4.

The RA does a check of the presented documents and attestations and makes sure that the collected information is complete and correct.

The RA will ensure that the assurance level of the enrolment process complies with the requirements for the ETSI standardized certificate policies, [ref. 2] for NCP+ and [ref. 1] and [ref. 3] for QCP-l & QCP-l-qscd.

Beforehand, the representative(s) of the Subscriber is informed of the personal data that is collected by the RA.

Where the private key is generated and installed on a Seal Creation Device not operated by ZETESCONFIDENS, for certificates compliant to NCP+ and QCP-l-qscd policy ZETESCONFIDENS shall check that the Seal Creation Device used has the security certification and (Q)SCD status in accordance with the certificate policy and ZETESCONFIDENS shall witness the key generation process and certificate request creation process. The CSR is included in the CSR form and witness report. The CSR form and witness report is signed by the ZETESCONFIDENS witness and the Certificate Manager.

For certificates compliant to QCP-l policy ZETESCONFIDENS is not obliged to attest the security certification of any Seal Creation Device used, nor witness the key generation process. ZETESCONFIDENS may witness the key generation process and certificate request creation process. If the latter is the case, the CSR form and witness report is signed by the ZETESCONFIDENS witness and the Certificate Manager. If not, only the CSR is stored.

4.1.2.3 The Subscriber Agreement

With the invitation to proceed in the enrolment, the Subscriber is supplied with reference in the model registration form to the following information:

- the privacy statement
- reference where to download the present CP, the CPS **[ref. 5]**, the TSPS **[ref. 4]** and the CTC [ref. 6]

The Registration Form serves as the Subscriber Agreement and is signed by an authorized representative of the Subscriber. This is considered the formal acceptance by the Subject/Subscriber whereby it accepts

- responsibility that the information provided by the Subscriber to the RA is correct, complete, valid and up to date,
- that the ZETESCONFIDENS maintains a retention period of 7 years after any certificate based on these records ceases to be valid of all the information pertaining to the registration and enrolment, the certificate request, the suspension/reactivation/revocation of the certificate,
- that in case ZETESCONFIDENS (as CA and RA) ceases its activities, this data may be transferred to a third party, respecting the same terms and conditions as defined in the Subscriber Agreement,
- acknowledges the rights, obligations and responsibilities of ZETESCONFIDENS and the other PKI Actors, as defined in the Subscriber Agreement and by law,
- the Subscriber has the obligation to inform ZETESCONFIDENS of any changes or events that may affect the validity or the content of the certificate,
- the issuance of a certificate of a specific type and policy with a certain content.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The RA verifies the content of the Registration Form and if applicable the CSR Form and witness report.

4.2.2 Approval or rejection of certificate applications

The RA may reject a request if the request cannot be authenticated or if the request does not comply with the rules and standards as defined for the type of certificate of for other reasons, at the discretion of and under the responsibility of ZETESCONFIDENS.

Accepted certificate requests are passed from the RA that formally formats the certificate request to the CA, to be ultimately processed by the CA system which must validate each request and may reject a certificate request if the request cannot be authenticated or if the request does not comply with the rules and standards as defined for the type of certificate, at the discretion of and under the responsibility of ZETESCONFIDENS.

4.2.3 Time to process certificate applications

No stipulations.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

For every certificate request, the CA will perform the following checks and actions:

- The CA will check that the request is from an approved Subscriber’s Certificate Manager.
- The CA will check the authorization for the type of request and refuse requests that pertain to certificate profiles for which the requester is not authorized.
- The CA matches the certificate request against a pre-defined certificate profile. The variable information in the request must match with the template and rule set of the certificate profile.

- The CA will add non-variable and variable information to the certificate, as defined in the certificate profile.

4.3.2 Notification of issuance of certificate

The Subscriber's Certificate Manager is notified of the issuance of the certificate by means of a signer Certificate Delivery Form.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

A certificate is deemed as accepted by the Subscriber upon the certificate's first use or in the absence of a rejection and revocation request within 1 working day after delivery of the certificate to the Subscriber's Certificate Manager, whichever comes first.

4.4.2 Publication of the certificate by the CA

The certificate is not published in a repository.

4.4.3 Notification of certificate issuance by the CA to other entities

The CA may also notify the Subscriber of the issuance of the certificate.

4.5 Key pair and certificate usage

4.5.1 Subject private key and certificate usage

The private keys and related certificates are to be used exclusively for the purposes described in section 1.4.

The Subject is bound by the usage conditions and obligations mentioned in the Subscriber Agreement, the CP and CPS, and the CTC. The Subject must protect its authentication means and any associated Activation Data or other information against loss, theft, disclosure, compromise or modification.

4.5.2 Relying Party public key and certificate usage

Relying Parties should not rely on the certificate unless they have performed the following actions:

- Evaluate whether the certificate is appropriate for the intended usage
- Restrictively accept the certificate only for the intended usage and for the appropriate applications, in compliance with the key usage information encoded in the certificate and in compliance with the limitation of use stated in the certificate (directly or through the referred CPS and CP).
- Successfully perform public key operations as a condition of relying on a certificate.
- Validate the certificate and each certificate in the certificate's trust hierarchy by using at least one of the mechanisms for certificate status information provided indicated in the certificate.
- If the certificate has been revoked, has been suspended or has expired the relying party must Immediately stop trusting the certificate, and must undertake the necessary checks and corrections with respect to prior use of the certificate in relation to the date and time and the nature of the certificate's change of status
- Take all other precautions with regards to the use of the certificate as set out in the Certification Practice Statement and the Certificate Policy,
- only rely on a certificate as may be reasonable under the circumstances.

4.6 Certificate renewal

Certificate renewal requires a new duly signed CSR form.

4.7 Certificate re-key

Certificate re-key requires a new duly signed CSR form.

4.8 Certificate modification

Certificate modification requires a new duly signed Registration Form and a new duly signed CSR form.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Under normal circumstances revocation is applied:

- If the Subscriber or the mandated certificate manager exercises his/her right for revocation of the certificate,
- If the information in the certificate is false, not correct or no longer valid,
- If there is reason to believe or suspect that the secret information pertaining to the Subject's authentication means has been compromised,
- If there is reason to believe that the certificate has been issued or used not in accordance with the applicable rules (e.g. rules expressed in the present document or in the CP have been violated),
- If the Subject is no longer capable of using the certificate,
- If the Subscriber decides that the Subject is no longer entitled to the certificate,
- If the private key was compromised,
- If the Seal Creation Device no longer has the required certification or QSCD status,
- in case of a court order,
- in case of termination of the trust service.

4.9.2 Parties that can request revocation

The CA can perform revocation in exceptional cases such as fraud, security compromise, non-compliance or for legal reasons.

The Subject or the Certificate Manager can request revocation for reasons internal to the Subject.

4.9.3 Procedure for revocation request

Revocation requests are submitted to the SRA. Procedures used for certificate revocation request are referenced in the Subscriber Agreement.

4.9.4 Revocation request grace period for the Subscriber/Subject

A Subscriber is required to request revocation of a certificate immediately upon discovering a reason for revocation of the certificate.

4.9.5 Time within which CA must process the revocation request

Revocation requests shall be processed at the latest 24 hours following receipt of the request.

4.9.6 Revocation checking obligations for Relying Parties

Relying parties must use at least one of the certificate status services that are indicated in the certificate. If the preferred service is unavailable, then the Relying Party is responsible for exhausting all other services. The Relying Party is responsible for making the final decision whether to trust the certificate, regardless of the availability of the certificate status information services.

4.9.7 CRL issuance frequency

See the Certification Practice Statement **[ref 5]**.

4.9.8 Maximum latency for CRLs

See the Certification Practice Statement **[ref 7]**

4.9.9 On-line revocation/status checking availability

See section 4.10 for more information.

4.9.10 Requirements on Relying Parties to perform on-line revocation checking

ZETESCONFIDENS maintains an Online Certificate Status Protocol (OCSP) service free of charge for use by Subjects and free of charge for normal use by Relying Parties. The free OCSP service is accessible without client authentication and accepts unsigned requests. See section 2.4 for information on Access Control and Restrictions regarding the use of the OCSP service.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

No stipulations.

4.9.13 Circumstances for suspension

Not applicable. ZETESCONFIDENS reserves the right to enhance the policy in the future to introduce certificate suspension.

4.9.14 Who can request suspension

Not applicable. ZETESCONFIDENS reserves the right to enhance the policy in the future to introduce certificate suspension.

4.9.15 Procedure for suspension request

Not applicable. ZETESCONFIDENS reserves the right to enhance the policy in the future to introduce certificate suspension.

4.9.16 Limits on suspension period

Not applicable. ZETESCONFIDENS reserves the right to enhance the policy in the future to introduce certificate suspension.

4.10 Certificate status services

4.10.1 Operational characteristics

CRL and delta-CRL download service

CRLs and delta -CRLs are renewed at regular intervals before the expiration dates. CRLs or delta-CRLs may be renewed ad hoc. For qualified certificates the CRLs maintain the information on revoked certificates also after the expiration of those certificates. The delta-CRL service is optional and certificates do not necessarily include the delta-CRL URL.

OCSP service

The OCSP service is available for unsigned requests and is synchronised with the latest certificate status information. The OCSP infrastructure consists of multiple OCSP responders which are accessible via a common URL. The OCSP responses are signed by an OCSP responder signing key. The OCSP responder signing certificate is issued by the corresponding CA. The OCSP service is optional and certificates do not necessarily include the OCSP URL.

Retention period for Certificate Status Information after expiration of the certificates

CRLs will contain certificate status information for qualified certificates also beyond the expiration date of the certificate.

4.10.2 Service availability

Certificate status services are maintained at least until all the certificates have either expired or have been revoked.

In case of unavailability due to an act of God, failure of infrastructure outside the control of ZETESCONFIDENS or any other reason, Zetes shall make best endeavours to reinstate availability of the service within 5 working days.

4.10.3 Optional features

No stipulations.

4.11 End of subscription

The termination of a subscription is defined in the Subscriber Agreement.

These agreements define:

- the terms and conditions
- the actions to be undertaken to initiate termination
- the actions to be undertaken upon termination

Upon termination of the subscription, the certificates issued on behalf of the Subscriber will be revoked.

4.12 Key escrow and recovery

Not applicable. The intended usage is electronic seal with non-repudiation. Key escrow and key recovery are not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

For the facility, management and operational controls for the CA, RA and other PKI components refer to section 5 of the general Trust Services Practice Statement [ref. 4] for:

- Facility, management and operational controls (i.e. physical controls, procedural controls and personnel controls),
- Provisions on security compromise and disaster recovery, and on termination of all or parts of the trust service activities.

Each Subscriber is responsible for its own facility, management and operational controls.

6. TECHNICAL SECURITY CONTROLS

This section covers the technical security controls for the end entity key pair on a Seal Creation Device owned by the Subscriber.

For the technical security controls (including key management) for the CA, RA and other PKI components refer to section 6 of the general Trust Services Practice Statement [ref. 4].

6.1 Key pair generation and installation

6.1.1 Key generation for the Subject

(Q)SCD not operated by Zetes.

The key generation process is performed by the Subject and (where applicable) controlled through witnessing by the ZETESCONFIDENS, according to the registration procedure described in section 4.1.2.2.

6.1.2 Private key delivery to the Subject

See 6.1.1.

6.1.3 Public key delivery to certificate issuer

The public key is delivered to the certificate issuer by means of a signed CSR Form.

6.1.4 CA public key delivery to Relying Parties

The ZETESCONFIDENS CA certificates shall be published on https://repository.confidens.zetes.com. See section 6 of the general Trust Services Practice Statement [ref. 4].

Subscribers may provide the CA certificates to Relying Parties by including said certificates with the sealed data or by any other means that is fit for purpose.

6.1.5 Key sizes

The algorithms, protocols or key lengths must meet the recommendation of the edition of ETSI TS 119 312 at the time of the key creation for the intended purpose and the intended use period of the key.

6.1.6 Public key parameters generation and quality checking

The keys must be generated on a certified Seal Creation Device in accordance with the device’s usage conditions for certified use. Public key parameters are generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. RSA keys must use the public exponent ‘010001’.

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

ZETESCONFIDENS ensures that the key usage properties encoded in the certificates correspond with the intended use of the certificates as described in the present document..

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Where the applicable certificate policy is QCP-l-qscd, the Cryptographic Module complies with the requirements for a Qualified Signature and Seal Creation Device (QSCD) as specified in Regulation (EU) No 910/2014 -- Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (eIDAS) pursuant to article 39 paragraph 2.

6.2.2 Private key multi-person control

Not applicable for the Subject Private Key.

6.2.3 Private key escrow / backup / archival

Private key backup and archival is allowed and is subject to the Subject’s key backup and archival policy.

For certificates under NCP+ and QCP-l-qscd, private keys cannot be extracted in non-encrypted format from the HSM or SCD on which they are generated. Extraction of private keys in encrypted form is possible and may be used for backup & restore purposes and/or for high-availability purposes:

- restore for recovery in case of failure of the infrastructure
- restore in case of replacement of an existing HSM
- initializing additional HSMs to expand the infrastructure’s capacity
- high-availability clusters or site fail-over setups

6.2.4 Private key transfer into or from a cryptographic module

Private key transfer is allowed and is subject to the Subject’s key policy.

For certificates under NCP+ and QCP-l-qscd, private keys are generated on-board the (Q)SCD and can be transferred to another (Q)SCD in accordance with Section 6.2.3. Subscribers must use an (Q)SCD in accordance with the certification requirements of the ETSI 319 411 certificate policy for NCP+ and QCP-l-qscd respectively.

6.2.5 Private key storage on cryptographic module

Private key storage is subject to the Subject’s key policy.

For certificates under NCP+ and QCP-l-qscd, private keys are stored on-board the (Q)SCD and used on-board the (Q)SCD. Subjects must use an (Q)SCD in accordance their internal policies and the official certification requirements of the (Q)SCD.

6.2.6 Method for activating private keys

Responsibility for private key management is left under the control of the Subject.

6.2.7 Method of deactivating private key

Responsibility for private key management is left under the control of the Subject.

6.2.8 Method of destroying private key

Responsibility for private key management is left under the control of the Subject.

6.2.9 Capabilities and Rating of the Cryptographic Module

For certificates under NCP+ and QCP-l-qscd, the Subscriber shall only use (Q)SCD that meet the requirements laid out for NCP+ or QCP-l-qscd policies. The Subscriber is responsible for using certified (Q)SCD.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are archived by the CA in the form of the certificates that contain the public key. See section 6 of the general Trust Services Practice Statement [ref. 4]. Subscribers may archive the public keys in the form of the certificates or in other forms.

6.3.2 Certificate operational periods and key pair usage periods

No stipulations.

6.4 Activation data

The Subject is responsible for choosing activation data and providing natural persons or devices access under their care. For certificates under NCP+ and QCP-l-qscd, Subjects must use a (Q)SCD in accordance their internal policies and the official certification requirements of the (Q)SCD.

6.5 Computer security controls

The Subject is responsible for the controls of the IT environment in which the private key and when applicable the (Q)SCD are used.

6.6 Life cycle technical controls

The Subject is responsible for the controls of the IT environment in which the private key and when applicable the (Q)SCD are used.

6.7 Network security controls

The Subject is responsible for the controls of the IT environment in which the private key and when applicable the (Q)SCD are used.

6.8 Time-stamping

The Subscriber is recommended to use a UTC coordinated time source such as but not limited to the NTP service of the Royal Observatory of Belgium.

7. PROFILES

7.1 Certificate profiles

The certificates adhere to the industry standards ISO/IEC 9594-8 / ITU X.509 and ETSI EN 319 412 part 1, 3 and 5.

7.1.1 The CA hierarchy

The CA hierarchy is the following:

CN=ZETES TSP Root CA 001, C=BE, O= ZETES SA (VATBE-0408425626)

```
|     subject serial number =        001
|     certificate serial number =    02 54 1A A9 50 D7 CE 1F
|     SHA1 thumbprint =              37 53 D2 95 FC 6D 8B C3 9B 37 56 50 BF FC 82 1A ED 50 4E 1A
|
----  ZETES TSP Qualified CA 001  (extended validity until 20/05/2031)
        Subject serialNumber =       001
        certificate serial number =  71 D6 DA E3 C4 5D D4 AD
        SHA1 thumbprint =            D2 80 F6 69 54 A6 81 53 66 DD DA 09 32 5D 02 6F 77 75 82 27
```

The CA hierarchy and the associated CA certificate profiles, OCSP certificate profile and CRL profiles are described in detail in the Certification Practice Statement documents.

7.1.2 Certificate Profile for Advanced Electronic Seal based on NCP+

This certificate profile is for certificates issued in accordance with the NCP+ certificate policy and complies with ISO/IEC 9594-8 / ITU X.509 and ETSI EN 319 412-1/3.

Table 1 Certificate profile for Advanced Electronic Seal (NCP+)

Certificate profile conforming to ETSI NCP+ version 1.0			
ATTRIBUTES			
Version		-	**0x02** *(= X.509 certificate version 3)*
Serial Number		-	**XXXXXXXXXXXXXXXXXX** < 64-bit random number > compliant with CA/B Forum requirements, validated to ensure uniqueness of the certificate serial number, compliant with RFC 5280 and X.690
Signaturealgorithm	**algorithm**	-	**sha256WithRSAEncryption**
Signature Value		-	< the signature created by the CA >
SubjectPublicKeyInfo	**algorithm**	-	**RSA2048**
	subjectPublicKey	-	value of the public key
Validity	**notBefore**	-	variable (key generation date and time or later)
	notAfter	-	variable
Issuer	**serialNumber**	-	as in the issuing CA certificate
	commonName	-	as in the issuing CA certificate
	organizationName	-	as in the issuing CA certificate
	countryName	-	as in the issuing CA certificate
Subject	**commonName**	-	variable, mandatory, ETSI TS 319 412 part 3 name commonly used by the subject to represent itself
	locality		variable, optional
	countryName	-	variable, mandatory, ETSI TS 319 412 part 3
	organizationName	-	variable, mandatory ETSI TS 319 412 part 3 full registered name of the subject (legal person)
	organizationIdentifier	-	variable, mandatory ETSI TS 319 412 part 3
	organizationalUnitName	-	variable, optional
EXTENSIONS -- Authority Properties			
authorityKeyIdentifier	**keyIdentifier**	-	< SHA-1 hash of the public key of the CA (as specified in RFC 5280) >
authorityInfoAccess	**accessMethod**	**-**	**OID 1.3.6.1.5.5.7.48.2** {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) caIssuers(2)}
	accessLocation	**-**	**http://crt.confidens.zetes.com/ZETESTSPQUALIFIEDCA001.crt**
	accessMethod	**-**	**OID 1.3.6.1.5.5.7.48.1** (optional) {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
	accessLocation	**-**	**http://ocsp.confidens.zetes.com** (optional)
CRLDistributionPoint	**distributionPointName**	-	**-**
	fullname	-	**http://crl.confidens.zetes.com/ZETESTSPQUALIFIEDCA001.crl**
FreshestCRL	**distributionPointName**	-	**-**
	fullname	-	**http://crl.confidens.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl**
EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	**keyIdentifier**	-	< 4-bit value 0I00 + least significant 60 bits of the SHA-1 hash of the value of subjectPublicKey bit string (tag, excluding the length and number of unused bit-string bits), as specified in RFC 5280 >
EXTENSIONS -- Policy Properties			
keyUsage	**nonrepudiation**	c	ETSI EN 319 412 part 2 chapter 4.3.2 key usage type A
certificatePolicies	**policyIdentifier**	-	ZETESCONFIDENS Policy Identifier: **OID 1.3.6.1.4.1.47718.2.32.2021.1.3.20.1112.3.2**
	policyQualifierId	-	Id-qt-1 (**CPS**)
	Qualifier	-	**https://repository.confidens.zetes.com/**
	policyIdentifier	-	ETSI Policy Identifier: **OID 0.4.0.2042.1.2** (NCP+)
basicConstraints	**subjectType**	c	**False** (CA = false)

7.1.3 Certificate Profile for Advanced Electronic Seal based on QCP-l

Certificates issued under these requirements are aimed to support the advanced electronic seals based on a qualified certificate defined in articles 36 and 37 of the Regulation (EU) No 910/2014 [Ref. 1]. This certificate profile is for certificates issued in accordance with the QCP-l certificate policy and complies with ISO/IEC 9594-8 / ITU X.509 and ETSI EN 319 412-1/3/5.

Table 2 Certificate profile for Advanced Electronic Seal with Qualified Certificate (QCP-l)

Certificate profile conforming to ETSI QCP-l version 1.0			
ATTRIBUTES			
Version		-	0x02 *(= X.509 certificate version 3)*
Serial Number		-	XXXXXXXXXXXXXXXXXX < 64-bit random number > compliant with CA/B Forum requirements, validated to ensure uniqueness of the certificate serial number, compliant with RFC 5280 and X.690
Signaturealgorithm	algorithm	-	sha256WithRSAEncryption
Signature Value		-	< the signature created by the CA >
SubjectPublicKeyInfo	algorithm	-	RSA2048
	subjectPublicKey	-	value of the public key
Validity	notBefore	-	variable (key generation date and time or later)
	notAfter	-	variable
Issuer	all fields	-	<as in the issuing CA certificate>
Subject	commonName	-	variable, mandatory, ETSI TS 319 412 part 3 name commonly used by the subject to represent itself
	locality		variable, optional
	countryName	-	variable, mandatory, ETSI TS 319 412 part 3
	organizationName	-	variable, mandatory ETSI TS 319 412 part 3 full registered name of the subject (legal person)
	organizationIdentifier	-	variable, mandatory ETSI TS 319 412 part 3
	organizationalUnitName	-	variable, optional
EXTENSIONS -- Authority Properties			
authorityKeyIdentifier	keyIdentifier	-	< SHA-1 hash of the public key of the CA (as specified in RFC 5280) >
authorityInfoAccess	accessMethod	-	OID 1.3.6.1.5.5.7.48.2 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) caIssuers(2)}
	accessLocation	-	http://crt.confidens.zetes.com/ZETESTSPQUALIFIEDCA001.crt
	accessMethod	-	OID 1.3.6.1.5.5.7.48.1 (optional) {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
	accessLocation	-	http://ocsp.confidens.zetes.com (optional)
CRLDistributionPoint	distributionPointName	-	-
	fullname	-	http://crl.confidens.zetes.com/ZETESTSPQUALIFIEDCA001.crl
FreshestCRL	distributionPointName	-	-
	fullname	-	http://crl.confidens.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl
EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	keyIdentifier	-	< 4-bit value 0I00 + least significant 60 bits of the SHA-1 hash of the value of subjectPublicKey bit string (tag, excluding the length and number of unused bit-string bits), as specified in RFC 5280 >
EXTENSIONS -- Policy Properties			
keyUsage	nonrepudiation	c	ETSI EN 319 412 part 2 chapter 4.3.2 key usage type A
certificatePolicies	policyIdentifier	-	ZETESCONFIDENS Policy Identifier: OID = 1.3.6.1.4.1.47718.2.32.2022.1.7.20.1112.3.2
	policyQualifierId	-	Id-qt-1 (CPS)
	Qualifier	-	https://repository.confidens.zetes.com/
	policyIdentifier	-	ETSI Policy Identifier: OID = 0.4.0.194112.1.1 (QCP-l)
basicConstraints	subjectType	c	False (CA = false)
qcStatement			OID: 1.3.6.1.5.5.7.1.3
	qcCompliance	-	OID: 0.4.0.1862.1.1 {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1)}
	qcType	-	OID: 0.4.0.1862.1.6 {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcType(6)}
	qcTypeEseal	-	OID: 0.4.0.1862.1.6.2 {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcType(6) qct-eseal(2)}
	SemanticsId-eIDASLegal	-	OID: 0.4.0.194121.1.4 (optional) {itu-t(0) identified-organization(4) etsi(0) id-cert-profile(194121) id-etsi-qcs-semantics-identifiers(1) id-etsi-qcs-SemanticsId-eIDASLegal(4)}
QcPDS	PdsLocations	-	OID: 0.4.0.1862.1.5 sequence of 1 or more sets of language code + URL
	url	-	https://pds.confidens.zetes.com
	language code	-	ISO 639-1 language code EN

7.1.4 Certificate Profile for Qualified Electronic Seal based on QCP-l-qscd

This certificate profile is for certificates issued in accordance with the QCP-l-qscd certificate policy and complies with ISO/IEC 9594-8 / ITU X.509 and ETSI EN 319 412-1/3/5.

Table 3 Certificate profile for Qualified Electronic Seal with QSCD and QC

Certificate profile conforming to ETSI QCP-l-qscd version 1.0			
ATTRIBUTES			
Version		-	0x02 *(= X.509 certificate version 3)*
Serial Number		-	XXXXXXXXXXXXXXXXXX < 64-bit random number > compliant with CA/B Forum requirements, validated to ensure uniqueness of the certificate serial number, compliant with RFC 5280 and X.690
Signaturealgorithm	algorithm	-	sha256WithRSAEncryption
Signature Value		-	< the signature created by the CA >
SubjectPublicKeyInfo	algorithm	-	RSA2048
	subjectPublicKey	-	value of the public key
Validity	notBefore	-	variable (key generation date and time or later)
	notAfter	-	variable
Issuer	all fields	-	<as in the issuing CA certificate>
Subject	commonName	-	variable, mandatory, ETSI TS 319 412 part 3 name commonly used by the subject to represent itself
	locality		variable, optional
	countryName	-	variable, mandatory, ETSI TS 319 412 part 3
	organizationName	-	variable, mandatory ETSI TS 319 412 part 3 full registered name of the subject (legal person)
	organizationIdentifier	-	variable, mandatory ETSI TS 319 412 part 3
	organizationalUnitName	-	variable, optional
EXTENSIONS -- Authority Properties			
authorityKeyIdentifier	keyIdentifier	-	< SHA-1 hash of the public key of the CA (as specified in RFC 5280) >
authorityInfoAccess	accessMethod	-	OID 1.3.6.1.5.5.7.48.2 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) caIssuers(2)}
	accessLocation	-	http://crt.confidens.zetes.com/ZETESTSPQUALIFIEDCA001.crt
	accessMethod	-	OID 1.3.6.1.5.5.7.48.1 (optional) {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
	accessLocation	-	http://ocsp.confidens.zetes.com (optional)
CRLDistributionPoint	distributionPointName	-	-
	fullname	-	http://crl.confidens.zetes.com/ZETESTSPQUALIFIEDCA001.crl
FreshestCRL	distributionPointName	-	-
	fullname	-	http://crl.confidens.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl
EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	keyIdentifier	-	< 4-bit value 0100 + least significant 60 bits of the SHA-1 hash of the value of subjectPublicKey bit string (tag, excluding the length and number of unused bit-string bits), as specified in RFC 5280 >
EXTENSIONS -- Policy Properties			
keyUsage	nonrepudiation	c	ETSI EN 319 412 part 2 chapter 4.3.2 key usage type A
certificatePolicies	policyIdentifier	-	ZETESCONFIDENS Policy Identifier: OID = 1.3.6.1.4.1.47718.2.32.2022.1.6.21.1112.3.2
	policyQualifierId	-	Id-qt-1 (CPS)
	Qualifier	-	https://repository.confidens.zetes.com/
	policyIdentifier	-	ETSI Policy Identifier: OID = 0.4.0.194112.1.3 (QCP-l-qscd)
basicConstraints	subjectType	c	False (CA = false)
qcStatement			OID: 1.3.6.1.5.5.7.1.3
	qcCompliance	-	OID: 0.4.0.1862.1.1 {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1)}
	qcType	-	OID: 0.4.0.1862.1.6 {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcType(6)}
	qcTypeEseal	-	OID: 0.4.0.1862.1.6.2 {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcType(6) qct-eseal(2)}
	qcSSCD	-	OID: 0.4.0.1862.1.4 {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) QcSSCD(4)}
	SemanticsId-eIDASLegal	-	OID: 0.4.0.194121.1.4 (optional) {itu-t(0) identified-organization(4) etsi(0) id-cert-profile(194121) id-etsi-qcs-semantics-identifiers(1) id-etsi-qcs-SemanticsId-eIDASLegal(4)}
QcPDS	PdsLocations	-	OID: 0.4.0.1862.1.5 sequence of 1 or more sets of language code + URL
	url	-	https://pds.confidens.zetes.com
	language code	-	ISO 639-1 language code EN

7.1.5 Certificates for Test Purposes

ZETESCONFIDENS may provide certificates for test purposes to allow Subscribers or third parties to check and test the various certificate types. Such test certificates may be made available on demand or in the public repository. Test certificates can be made available in a variety of certificate status conditions (valid, expired and revoked).

Test certificates clearly indicate that these are for testing purposes only:

- **subject name text fields** are prefixed with "TEST"
- in the **Subject Organization Identifier field**, in the identifier part, all digits are replaced by 0
- special **URL**s in test certificates:
  - http://crt.test.confidens.com/...
  - http://ocsp.test.confidens.com
  - http://crl.test.confidens.com/...
- unchanged **URLs** in test certificates:
  - https://repository.confidens.zetes.com
- **generic policy identifiers (OID)**: no differences, to allow testing whether 3rd party commercial applications correctly interpret and display these standardized generic OIDs
- **proprietary policy identifiers (OID):** are pre-fixed with the value "2.999."
- **Extra Policy field with User Notice text "This is a TEST certificate" identified under the test proprietary OID.**

(1) The URLs in the test certificates that refer to the CRL, the CA-certificate download and the OCSP service might be different from the equivalent in the real certificates. Under normal conditions, these URLs shall be mapped to the same resource as the URLs in the real certificates, to allow for testing with the production infrastructure. At the discretion of ZETESCONFIDENS these URLs may be diverted to another resource or dropped, e.g. to counter abusive or disruptive use of the test certificates.

(2) The repository URL remains identical as in production certificates because the test certificate must point to the real CP/CPS which also contain the information about the test certificates.

7.2 OCSP certificate profile

See the Certification Practice Statement **[ref 5]**.

7.3 CRL profile

See the Certification Practice Statement **[ref 5]**.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The ZETESCONFIDENS Trust Services Practice Statement [ref. 4] applies.

ZETESCONFIDENS PMA organizes with regards to its CA activities a compliance audit to ensure that it meets requirements, standards, procedures and service levels according to this document.

9. OTHER BUSINESS AND LEGAL MATTERS

The ZETESCONFIDENS Trust Services Practice Statement [ref. 4] applies.

The CP, CPS and the Subscriber Agreement constitute the main set of terms and conditions for the provision and use of this CA offering.

The Subscriber Agreement also contains the Certificate Terms and Conditions for the use of the Certificates under this CP.

A Relying Party can rely on all information available in the CPS and the CP. The Relying Party shall be deemed to have tacitly accepted the terms and conditions incorporated in the relevant public documents upon relying on the Certificate.

---------------------------LAST PAGE OF THIS DOCUMENT---------------------------