ZETES TSP QUALIFIED CA 001

CERTIFICATE POLICY FOR SIGNATURE CREATION SERVICE CERTIFICATES

Certificate Policy for certificates

for the ZetesConfidens Signature Creation Service

Publication date :	**03/09/2020**	
Effective date :	**04/09/2020**	
CP OID :	**1.3.6.1.4.1.47718.2.1.2.2.4.1 for LCP certificates** **1.3.6.1.4.1.47718.2.1.2.2.4.2 for NCP+ certificates** **1.3.6.1.4.1.47718.2.1.2.2.4.3 for QCP-n-qscd certificates**	
Version :	**1.2**	**01/09/2020**

Table of Content

Tables

ABOUT ZETES

Founded in 1984, Zetes NV/SA is a company incorporated in Belgium (European Union) and is part of the Zetes Group, which is fully owned by the Panasonic Group. Zetes NV/SA is active in the areas of identification documents, travel documents, smartcards, biometrics and trust services including the issuance of certificates.

In 2016, Zetes established an operational business unit within Zetes NV/SA to provide certificate services and other trust services for governments, the financial sector and private organizations. Since September 2018 these activities are marketed under the **ZetesConfidens** tradename (before referred to as "Zetes TSP").

All further references to "Zetes" in this document refer to the legal entity Zetes NV/SA unless explicitly stated otherwise.

Zetes NV/SA is registered in Belgium as follows:

In Dutch:	In French:
Zetes NV Straatsburgstraat 3 1130 Brussel België KBO 0408.425.626 BTW BE 0408 425 626	**Zetes SA** 3, Rue de Strasbourg 1130 Bruxelles Belgique BCE 0408.425.626 TVA BE 0408 425 626

ABOUT THIS DOCUMENT

Scope

The present document is the Certificate Policy (CP) document for Zetes TSP Qualified CA 001 for the issuance of certificates for the ZetesConfidens - Signature Creation Service.

This CA and the associated Signature Creation Service support

- Advanced Electronic Signature (AdES) meeting the requirements of Regulation (EU) No 910/2014 **[ref. 1]** and the requirements of ETSI EN 319 411-1 [LCP] and [NCP+] Certificate Policies (CP) **[ref. 2]**.
- Qualified Electronic Signature (QES) meeting the requirements of Regulation (EU) No 910/2014 **[ref. 1]** and the requirements of ETSI EN 319 411-2 [QCP-n], [QCP-l], [QCP-n-qscd] and [QCP-l-qscd] Certificate Policies (CP) **[ref. 6]**.

Intellectual Property Rights

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] ZETESCONFIDENS Certificate Terms and Conditions (CTC)

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

[ref. 5] ZETESCONFIDENS Signature Creation Service Practice Statement

[ref. 6] 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. 7] ZETESCONFIDENS Certificate Practice Statement for Zetes TSP Qualified CA 001

Document Version History

Version	Publication Date	Effective Date	Information about this Version
1.2	03/09/2020	04/09/2020	Update of the certificate profile. Update in descriptions of the RA and SRA roles to make the distinction between these roles clearer and to clarify that RA and SRA are different entities. Chapters 4.6 – 4.9 regarding certificate lifecycle contain new stipulations.
1.1	24/07/2020	28/07/2020	Update CP OIDs----------
1.0	24/02/2020	24/02/2020	First publication----------

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, in the capacity of QTSP, offers a Signature Creation Service. This service manages electronic signature creation data on behalf of the subjects on a qualified signature creation device (QSCD). This Signature Creation Service is described in the ZETESCONFIDENS Signature Creation Service Practice Statement **[ref. 5]**. The subject key generation is under the responsibility of this Signature Creation Service as well as the private key protection that is under the sole control of the subject.

This associated Signature Creation Service operates a centralized HSM-based qualified signature creation device (QSCD) in the sense of the Regulation (EU) No 910/2014 **[ref. 1].** The QSCD is used for cryptographic key generation and cryptographic signatures in combinations with a variety of certificate types and certificate policies.

The CA that is the object of the present document issues signature certificates for keys that are created and managed by said Qualified Signature Creation Devices.

ZETESCONFIDENS is the Trust Service Provider (TSP) and has final and overall responsibility for the provision of the ZETESCONFIDENS certificates offering for ZETESCONFIDENS Signature Creation Services, namely:

- Registration service through the ZETESCONFIDENS Registration Authority network of subordinate and local RAs: verifies the identity and if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.
- Certificate generation service through the ZETESCONFIDENS Certification Authority (CA) for Signature Creation Service: creates and signs certificates based on the identity and other attributes verified by the registration service.
- Key generation service on the QSCD infrastructure hosted and managed by ZETESCONFIDENS.
- Dissemination service for certificates, public terms and conditions, policy and practice information, to subjects, subscribers and relying parties.
- Revocation management service through the ZETESCONFIDENS Suspension and Revocation Authority network of Subordinate and local SRAs: 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 for server signing issued by the CA

The provision and use of Certificates issued under this policy are governed by the following documents:

- the present document
- **[ref. 2]** ETSI EN 319 411-1
- **[ref. 6]** ETSI EN 319 411-2
- **[ref. 3]** ZETESCONFIDENS Certificate Terms and Conditions (CTC)
- **[ref. 4]** ZETESCONFIDENS Trust Services Practice Statement (TSPS)

The present document states the practices to issue Certificates to natural persons. Common trust service provisioning practices non-specific to the issuance of such certificates, are provided in [ref. 4] and endorsed in the present practices by reference.

The relevant requirements of ETSI EN 319 411 part 1 and 2 are endorsed by the present document. The CA adheres to the certificate policies and certificate profiles as defined in ETSI EN 319 411 part 1 and 2 and as defined in ETSI EN 319 412 part 1 to 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 OID**	**Policy Description**
ETSI QCP-n-qscd	0.4.0.194112.1.2	Policy conforming to ETSI EN 319-411-2 for Qualified Certificates issued to natural persons, including the requirements with regards to the use of a Qualified Signature Creation Device.
ETSI NCP+	0.4.0.2042.1.2	Policy conforming to ETSI EN 319 411-1 for Enhanced Normalized Certificates issued to natural persons requiring the use of a Secure Cryptographic Device.
ETSI LCP	0.4.0.2042.1.3	Policy conforming to ETSI EN 319 411-1 for lightweight certificates for use cases with less stringent Subject registration-related requirements.

Corresponding Zetes proprietary Certificate Policy OID

Certificate policy	**ETSI Certificate Policy OID**	**Zetes Certificate Policy OID**
ETSI QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47718.2.1.2.2.4.3
ETSI NCP+	0.4.0.2042.1.2	1.3.6.1.4.1.47718.2.1.2.2.4.2
ETSI LCP	0.4.0.2042.1.3	1.3.6.1.4.1.47718.2.1.2.2.4.1

The CA conforms to the requirements pertaining to the most constringent policies. The main criterion that determine if a certificate conforms to a specific policy is the procedure for the registration of the Subject. The present document allows several registration sources, according to the procedure observed by the SUB-RA and its related L-RAs, as stated in the Subscriber contracts.

A Subscriber contract is necessarily bound to a certificate policy, according to the Registration procedure the Subscriber is supporting.

Qualified certificates and NCP+ certificates are only issued to Subscribers whose Subjects are identified with physical presence in front of the L-RA or the SUB-RA or by means of a registration procedure that is equivalent to a face to face registration procedure.

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

This document is called the "Zetes TSP Qualified CA - Certificate Policy for Server Signing certificates" and covers 3 different certificate policy OIDs :

- 1.3.6.1.4.1.47718.2.1.2.2.4.1 for LCP certificates
- 1.3.6.1.4.1.47718.2.1.2.2.4.2 for NCP+ certificates
- 1.3.6.1.4.1.47718.2.1.2.2.4.3 for QCP-n-qscd certificates

1.3 PKI participants

The PKI participants are all the legal entities or (associations of) natural persons who are involved in any of the processes and activities of ZETESCONFIDENS as a Trust Service Provider (TSP) and/or who are impacted by the use of certificates issued by ZETESCONFIDENS. All participants adhere to or are bound by the CP-CPS and CTC. The PKI participants involved in any of the processes and activities of ZETESCONFIDENS are also called PKI Actors.

PKI participants are defined as follows:

Subscribers	An organisation that enters into a contractual agreement with ZETESCONFIDENS on behalf of Subjects.
Subjects	Natural persons whose identity or identifier is encoded in the end user certificate issued by a CA. A Subject adheres to a Subscriber.
Relying Parties	Parties who rely on the validity of the certificate issued by the CA, e.g. for authentication or for validation of a transaction or document.
CA - Certification Authority	The entity issuing certificates to Subjects on request of the RA
RA - Registration Authority	ZETESCONFIDENS is the RA. The RA is the legal entity responsible for the supervision and control of all registration activities.
C-RA - Central Registration Authority	ZETESCONFIDENS is the Central Registration Authority. The C-RA is the organization and infrastructure within ZETESCONFIDENS that handles the registration and vetting of certificate requests received from the SUB-RAs. The C-RA also coordinates the certificate creation process between the QSCD management under the responsibility of the ZETESCONFIDENS Signature Creation Service and the Issuing CA.
SUB-RA - Subordinate Registration Authorities	The authority for the registration and vetting of Subjects and certificate requests for a specific Subscriber or group of Subscribers. The SUB-RA is either ZETESCONFIDENS or a designated legal entity (usually the Subscriber).
L-RA - Local Registration Authorities	The L-RA performs the front-office registration tasks and first-line vetting of Subjects. The L-RA is part of the SUB-RA.

SRA - Suspension and Revocation Authority	ZETESCONFIDENS is the SRA. The SRA is the entity responsible for the supervision and control of all certificate revocation and suspension activities.
Publication and Repository Services	ZETESCONFIDENS provides the publication and repository services. These services cover online publication of Certificate Practice Statements, Certificate Policies, terms and conditions, certificate validation data such as root certificates and certificate status information.

QSCD management	The Subject's key management is controlled by the ZETESCONFIDENS Signature Creation Service, that is in charge of key generation, key lifecycle management and key activation under control of the Subject. The CA and the Signature Creation Service are integrated with regard to the Subject's management (registration, enrolment, removal).

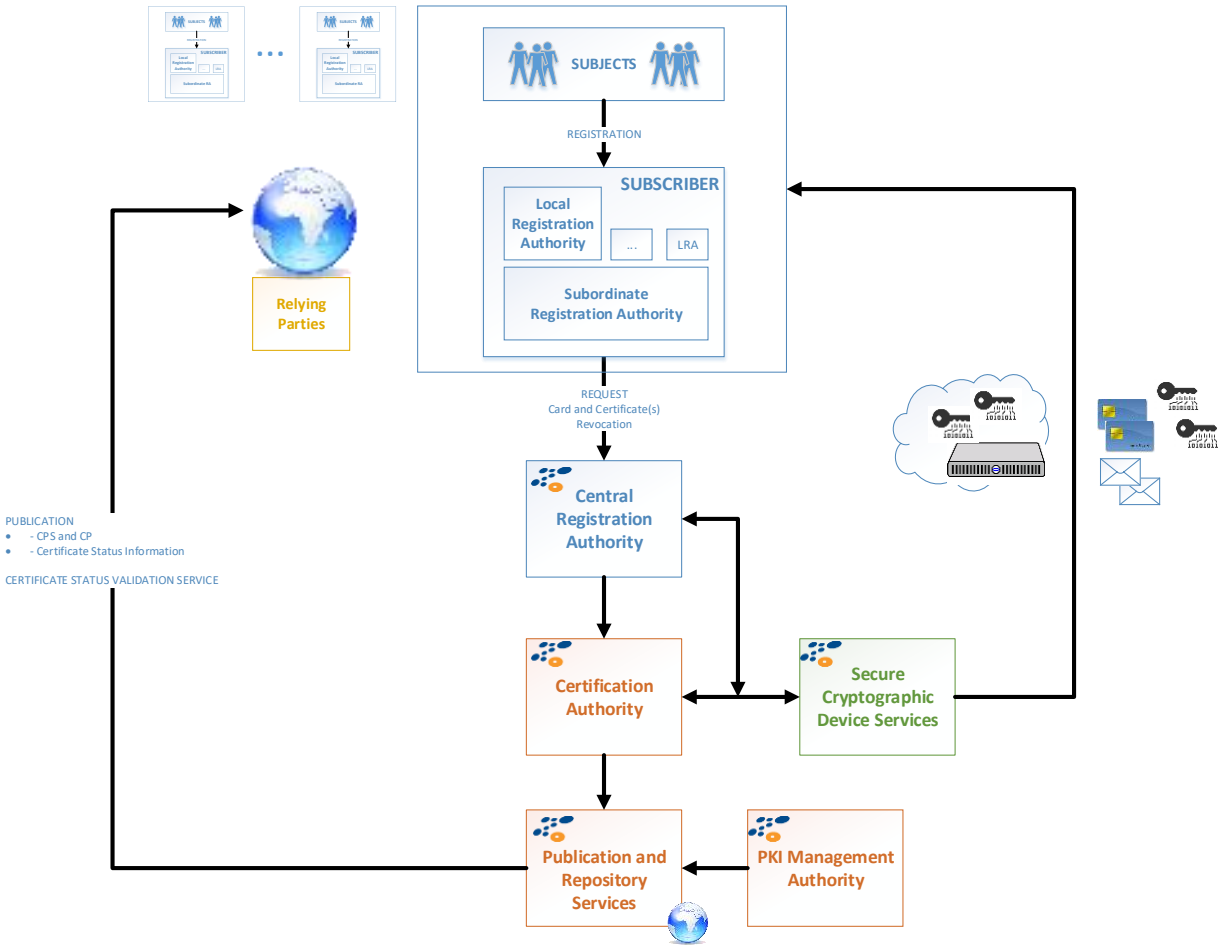

Figure 1 Diagram of the PKI participants

1.3.1 Certification Authority

ZETESCONFIDENS operates a CA hierarchy for issuing certificates to Subjects. The issuing CA is root-signed by the ZETES TSP ROOT CA 001.

The Certification Authority is responsible for:

- certificate creation and lifecycle changes
- certificate status information services
  - CRL
  - OCSP

1.3.2 Registration Authority (RA)

1.3.2.1 Overview

The Registration Authority is the entity that is responsible for enrolling subject for the Signature Creation Service. With regards to the issuance of certificates the RA is responsible for:

- The identification of the Subjects;
- Informing he Subjects about the CTCs;
- Authenticating and vetting certificate requests;
- Applying the naming conventions defined within this document when creating new entities, so that each entity is uniquely and unambiguously identified;
- Requesting the ZETESCONFIDENS Signature Creation Service to generate a key for the approved certificate application and to request the CAs to produce the certificates according to the relevant CP;
- Creating and maintaining an audit log of all significant events related to the RA's fulfilment of the above-mentioned responsibilities;
- Providing selective access to the audit log as specified in this document;
- Implementing other operational controls as specified in this document;
- Ensuring that the stored information and the applied processes are handled in a manner that is consistent both with the policies and procedures defined in this document.

The operational tasks of the RA are performed by the Central Registration Authority, one or more Subordinate Registration Authorities and their Local Registration Authorities as detailed in the next sub-sections. The RA also includes a supervisory body to supervise and audit the various other constituent parts of the RA.

1.3.2.2 Central Registration Authority (C-RA)

The Central RA is the organisational structure and the infrastructure of the RA within ZETESCONFIDENS that is tasked with the following duties:

- create a user profile for each Subject based on the information received from the SUB-RA
- process certificate requests originating from Subordinate RAs
- authenticate and validate the Subordinate RA and the certificate request itself
- act upon the result of this validation and, if approved,
    - select the appropriate Certificate Profile
    - interact with the ZETES Signature Creation Service for key generation and submission of a certificate request to the CA

The infrastructure for the Central RA is closely integrated with the ZETES Signature Creation Service:

- certificate requests are formally formatted by ZETES Signature Creation Service that generate the Subject's key pair and the interaction with the CA for obtaining the certificate(s) for a Subject is coordinated with the key generation process
- the vetting process for a enrolling a Subject on the ZETES Signature Creation Service relies on the vetting process for the associated certificate requests

The Central RA does not interact directly with a Subject except for matters related to incident management, exception management, or investigations .

1.3.2.3 Subordinate Registration Authorities (SUB-RA)

A Subordinate Registration Authority is the entity tasked with the organisation and the coordination of the registration process for a specific group of Subjects.

A Subordinate RA may delegate the actual registration process to one or more Local Registration Authorities.

The role of Subordinate RA can be performed by various parties such as:

- ZETESCONFIDENS
- the Subscriber
- an authorized third party.

The tasks of the SUB-RA are defined in internal documents when ZETESCONFIDENS is the SUB-RA, or in the RA contract when the SUB-RA is the Subscriber or an Authorized Third Party.

In most cases, the Subscriber assumes the role of Subordinate RA (see description of the Subscriber role).

The responsibilities of the SUB-RA are:

- to follow the registration process corresponding to the level of assurance required by the CP the SUB-RA is contractually bound (i.e. LCP, and/or NCP+).
- to ensure that the Subject has accepted the Subject Agreement

1.3.2.4 Local Registration Authorities (L-RA)

The Local RA is the organisation that is responsible for the actual registration of the Subject for whom the certificates are intended.

The Local RA can be part of the same legal entity as the Subordinate RA or can be a third party which is mandated by a Subordinate RA to register Subjects on its behalf.

The registration process is described in section 4 and in confidential documents that are internal to the TSP or where applicable part of the Subscriber agreement. The tasks, responsibilities and identity of the L-RA operators are defined in the Subscriber agreement.

1.3.3 Suspension and Revocation Authority

The Suspension and Revocation Authority is the entity that is responsible for executing certificate lifecycle changes on demand of the CA, the Subscriber or the Subject.

The SRA is responsible for:

- Processing certificate revocation requests within 24h of receipt;
- Authentication of certificate revocation requests stemming through authorised channels
- Requesting the CA to revoke the certificates for approved revocation application requests;

1.3.4 Subscriber and Subjects

1.3.4.1 Subscriber (organizations)

Subscribers are organisations who enter into a contractual agreement with Zetes for the purpose of using the Signature Creation Service, this includes issuing certificates to Subjects. A Subscriber must have a contractual agreement, membership agreement or some form of legal authority over the Subjects it represents.

Subscribers may request issuance, suspension, revocation or renewal of end-entity certificates for Subjects under their care, as defined by the contractual or legal relationship between Subscriber and Subject. The terms of this relationship can be reflected in the corresponding Subscriber Agreement.

The Subscriber's roles and responsibility are detailed in the Subscriber's agreement.

1.3.4.2 Subjects (natural persons)

Subjects are persons such as members, employees, participants, stakeholders, subordinates, customers, etc. who are represented by the Subscriber.

The Subject's roles and responsibility are detailed in the Certificate Terms and Conditions of use of ZETESCONFIDENS services (CTC, [ref 3].).

1.3.5 Relying parties

The Relying Parties are those parties who are relying on a ZETES Certificate for validating the identity of the Subject and a particular purpose or context as is indicated in the certificate. Relying Parties include other PKI participants or third parties.

1.3.6 Other participants

1.3.6.1 ZETES Signature Creation Service and QSCD management

The QSCD containing the private key corresponding with the certified public key is hosted and managed by the ZETESCONFIDENS Signature Creation Service.

Creation of keys for Subjects is performed by and under control of ZETESCONFIDENS Signature Creation Service. The private key is generated in the QSCD and cannot be used outside the QSCD nor without consent of the Subject.

The QSCD complies with the conditions defined in Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices (QSCD) pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014. ZETES shall monitor the QSCD certification status until the expiration of the last Certificate which was issued in conjunction with said Qualified SCD.

ZETESCONFIDENS will establish the necessary arrangements with the manufacturer or supplier of the QSCD to remain informed about any issues that might be relevant to the use or suitability of the QSCD.

If the certification of a Qualified SCD is withdrawn or for any other reason deemed inappropriate, ZETESCONFIDENS will take appropriate measures, taking into consideration security risks, liabilities and the consequences for the Subjects and Relying Parties. In such case, ZETESCONFIDENS reserves the right to terminate, deactivate, recall and/or destroy the affected devices and/or to revoke the affected certificates and/or to deactivate or destroy the affected keys. In such event, ZETES will notify the Belgian Supervisory Body and the implicated Subscribers.

1.3.6.2 Dissemination and Repository Services

ZETESCONFIDENS is responsible for operating the Dissemination Services (publication of Certification Practice Statement, TSP terms and conditions, CA certificates, certificate revocation lists and other related, public documents). This service also provides access to previous versions of these documents (Certification Practice Statement, TSP terms and conditions). Access to CRLs, CA Certificates and OCSP certificate status validation services is made available to all Relying Parties without restrictions. The Dissemination and Repository Services are provided as described in section 2 of the present Certification Practice Statement.

1.3.6.3 Revocation Management Services and Revocation Status Information Services

The CA is responsible for operating the Revocation Management Services and the Revocation Status Information Services (which provide Certificate validity status information) with regards to the ZETES Certificates. Other measures can be taken by ZETESCONFIDENS such as the destruction or the deactivation of the private key, of the user account, of the user access, etc. in parallel with the certificate revocation (see [ref. 5]).

1.3.7 ZETESCONFIDENS Policy Management Authority (PMA)

The PMA is the high-level management body that has overall responsibility for the TSP Services. The PMA responsibilities are detailed in the ZETESCONFIDENS Trust Services Practice Statement [ref. 4].

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The certificates issued under this policy are exclusively used by the ZETESCONFIDENS Signature Creation Service for the creation of electronic signatures 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 319 412-2
- 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 and the Subscriber to use certificates only according to the intended usage and restrictions of the present policy.

For validation of the electronic signature based upon a certificate issued under the present policy it is the responsibility of the Relying Party to use a software tool that correctly interprets, displays and uses the information and 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 Subscriber, 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.

The appropriate certificate usage is further clarified in the CTC.

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

See [ref. 4.]

1.5.2 Contact person

See [ref. 4.]

1.5.3 Person determining suitability for the policy

See [ref. 4.]

1.5.4 Approval procedures

See [ref. 4.]

1.6 Definitions and acronyms

1.6.1 Acronyms

ARL	Authority Revocation List
CA	Certificate Authority
CP	Certificate Policy

CPS	Certification Practice Statement
CRL	Certificate Revocation List
CTC	Certificate Terms and Conditions
DN	Distinguished Name
HSM	Hardware Security Module
IDP	Identity Provider
LCP	Lightweight Certificate Policy
LRA	Local Registration Authority
NCP	Normalized Certificate Policy
NCP+	(Extended) Normalized Certificate Policy (requiring a secure device)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority
QCP-l	Qualified Certificate Policy for certificates issued to legal persons
QCP-l-scd	QCP-l in combination with a Qualified Seal Creation Device
QCP-n	Qualified Certificate Policy for certificates issued to natural persons
QCP-n-qscd	QCP-n in combination with a Qualified Signature Creation Device
RA	Registration Authority
TSPS	Trust Services Practice Statement

1.6.2 Definitions

Activation Data	Data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorised use of the private key.
Certificate	A unit of information contained in a file that is digitally signed by the Certification Authority. It contains, at a minimum, the issuer, a public key, and a set of information that identifies the entity that holds the private key corresponding to the public key.
Certificate Revocation List	A signed list of identifiers of Certificates that have been revoked. Abbreviated as CRL. It is (periodically) made available by the CA to Subscribers and Relying Parties.
Certificate Terms and Conditions	These CTC are the specific terms and conditions part of the Subject Agreement that reiterate the terms and conditions for use of the Certificates by the Subject. They specifically reiterate the obligations applicable on the Subject as stated in ETSI EN 319 411 – part 1 and refer to the CPS and present CP.
Hardware Security Module (HSM)	Hardware Security Module. An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.
Lightweight Certificate LCP	A Certificate, issued under the by-default policy and security requirements for TSPs issuing certificates as defined in ETSI EN 319 411 – Part 1
Normalized Certificate NCP/NCP+	A Certificate issued under the policy and security requirements for TSPs issuing certificates as defined in ETSI EN 319 411 – Part 1, whereby the certification authority *may* support the same level of quality as for issuing Qualified Certificates, but "normalized" for wider applicability and for ease of alignment. The standard is applicable to the general requirements

	of certification in support of cryptographic mechanisms, including the general use of cryptography for authentication and encryption.
Qualified Certificate QCP-n, QCP-n-qscd QCP-l, QCP-l-qscd	A Certificate which meets the requirements laid down in Regulation (EU) No 910/2014 and Annex I thereof and is provided by a Qualified Trust Service Provider who fulfils the requirements laid down in the Regulation. The Regulation distinguishes between Qualified Certificates for different purposes: electronic signature, electronic seals, or website authentication. In the context of this document, the term Qualified Certificate will only reference to "qualified certificates for electronic signature" under the Regulation.
QSCD	Qualified Signature Creation Device
Relying party	Relying Parties are as defined in section 1.3.5
Subscriber	The Subscribers are as defined in section 1.3.4.1.
Secure Cryptographic Device	In the context of this document Secure Cryptographic Device refers to the QSCD managed by ZETESCONFIDENS Signature Creation Service.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ZETESCONFIDENS operates services 24/7 for the publication of information for Subscribers, Subjects and Relying Parties 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

Taking into account that

- 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 ZETESCONFIDENS Signature Creation Service applies protocols and formats electronic signatures that include the Subject's certificate chain with the signed data and thereby allows the Relying Party to retrieve the certificate from that source,
- The certificates contain privacy sensitive information,
- The act of publication or retraction of a certificate from a repository may in itself be privacy sensitive.

ZETESCONFIDENS as a matter of policy, does not publish certificates issued to Subjects (end entity certificates) in a public certificate repository. This policy is clearly stated in the contractual agreement with the Subscriber (if applicable). The ZETESCONFIDENS Signature Creation Service will include the end entity's certificate chain with the signed object. Relying parties need to consider the fact that end entity certificates will not be published in a public repository. 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

The CRLs or delta-CRLS are renewed before the CRL or delta-CRL is about to expire and may be renewed when certificates have been revoked. The CRL/delta-CRL is refreshed at least every 24 hours although the CRL validity (nextUpdate) may be set to a longer period.

For qualified certificates the CRLs maintain the information on revoked certificates also after the expiration of those certificates.

CRL publication is maintained until all certificates that were issued by the respective CA have expired.

Publication of terms and conditions, CPS, etc.

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 (see section 9.12).

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.

Subscribers, Subjects and Relying Parties have read-only access via the internet to all the repositories mentioned in 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

The name fields **givenName** and **surName** in the certificate for a natural person contain the official given names and surnames as stated on the person's birth certificate, identity card, passport or other acceptable breeder document.

For the purpose of conforming to ETSI EN 319 411-1 and to the requirements stated in the Regulation (EU) No 910/2014, the name attributes in the end entity certificates for natural persons are compliant with the ETSI EN 319 412 part 1 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 incorporate plain wording describing the intended usage or context of the certificate.

Certificate Attribute	Description
serialNumber	**Subject serial number or identifier**
givenName	**Official given name(s) of the Subject** as validated by the SUB-RA/L-RA. space (" ") separated full-form concatenation of given names, identical to how it is obtained from the identity document that was used to register the Subject
surName	**Official surname(s) of the Subject** as validated by the SUB-RA/L-RA. Space (" ") separated full-form concatenation of surnames, identical to how it is obtained from the identity document that was used to register the Subject
commonName	**Official name or calling name of the Subject + indication of the intended purpose for this certificate** The certificate will only contain one instance of commonName. The commonName is intended for a user friendly representation of the certificate holder's name.
Country	**Country of origin or country of residence** as validated by the SUB-RA/L-RA.
organizationName	**OPTIONAL - Official registered name of the Subscriber as a corporation or organization, including an official registered unique number or unique identifier of the Subscriber as a corporation or organization,** formatted as specified in ETSI EN 319 412-1 together with a semantic identifier. It is representing the registration number of the organization as stated in the official records.
organizational Unit	**OPTIONAL - The certificate may contain zero, one or more OU fields.** The OU field contains a proprietary identifier for an entity or category within the organizational structure of the Subscriber.
Title	**OPTIONAL - Official title of the Subject** as assigned by SUB-RA/L-RA.

3.1.2 Need for names to be meaningful

The names used in the certificates are normal given names and surnames for natural persons. See section 3.1.1.

3.1.3 Anonymity or pseudonymity of Subscribers

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 normal given names and surnames for natural persons. See section 3.1.1.

3.1.5 Uniqueness of names

Subject DNs are guaranteed to be unique. The subjectSerialNumber field of the Subject DN is assigned by the Subordinate RA to each Subject. The Subordinate RA guarantees that this field can only be linked to a single uniquely identifiable Subject.

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 SUB-RA.

3.2.1 Method to prove possession of private key

Proof of Possession of Private Key for Subjects

The key generation process is performed on ZETESCONFIDENS' Signature Creation Service QSCD complying with the conditions defined in Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014. Each generated key pair is uniquely associated with a Subject Profile by the Signature Creation Service. The certificate request is signed with the private key, proving the link with the public key to be certified. See also [**ref. 5**]

3.2.2 Authentication of organization identity

Organization acting as a Subscriber

Organizations acting as Subscriber are authenticated by ZETESCONFIDENS in accordance with the rules and regulations for the naming and identification of organizations as applicable in the Kingdom of Belgium or as applicable in the country where the PKI Participant is registered.

When the Subscriber Agreement is established, ZETESCONFIDENS verifies the organisation's relationship with the Subjects, in particular verifies the Subscriber's entitlement to facilitate and/or act on behalf of the Subject.

Organisational entities other than ZETES that are PKI Actors

Organization that are PKI Actors and have a role and responsibilities defined within the framework agreement (e.g. a Subordinate RA, a Local RA, a Subscriber representing a group of Subjects, etc.), are authenticated through procedures described in the relevant framework agreement conforming to the above paragraph.

3.2.3 Authentication of individual identity

Authentication of Identity for Subjects

For QCP-n-qscd and NCP+ the identity of a Subject is authenticated by the RA.

The procedure follows the steps described below:

1) STEP 1 – ENR 1: **creation of a registration file containing the subject's identification** information (name, surname, unique identifier when relevant, address, date of birth, contact information, authentication-related information, etc.); this file can be prepared on-line or at the occasion of step 2 below.

2) STEP 2 – ENR 2: **validation** that the above information is genuine and belongs to the person requesting access to the signing service.
   To do so:
   a) For QCP-n-qscd and NCP+, the SUB-RA (or its authorised L-RA) relies on a **face to face registration in person or equivalent** . The following methods are supported:
      (i) face to face:
      - the Subject will have to appear in person in front of an authorized operator of the Local RA and present a valid and authentic identity document (national identity card, residence permit, passport, etc.) to the Local RA operator to conclude the registration process. The Local RA operator validates the authenticity of the presented documents and checks that the individual is the genuine holder of the presented documents according to rules defined by ZETESCONFIDENS internal instructions and - optionally -

additional rules defined by the Subordinate RA and/or the Subscriber. Optionally, in addition to identifying and authenticating the Subject, the SUB-RA / L-RA validates the request and checks the Subject's entitlements
- The Subject profile is provided to the SUB-RA and transferred to the C-RA
- the Subject is provided with information about the service and credential for further authentication purposes.

(ii) equivalent to face to face:
- the SUB-RA relies on a IDP who performed a recent face to face validation of the subject's identity. E.g. Subjects who are holder of a Belgian electronic Identity Card or a Belgian electronic Residence Permit Card can use the SUB-RA online registration portal. Subjects authenticate (log on) with their eID card, which implies possession of the eID card and knowledge of the eID PIN code.
- the Subject profile is transferred to the C-RA
- the Subject is provided with information about the service and credential for further authentication purposes.

b) For LCP certificates, the registration method relies on the validation of an official form of identification that has at least the assurance level "substantial" as defined in Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

Example of a registration process for a SUB-RA:
- a signed recto-verso copy of the Subject's identity document is provided through the SUB-RA online registration portal, together with other information provided by the subject (e.g. the mobile phone number and e-mail address).
  The SUB-RA verifies the validity of the identity document (e.g. using the Belgian federal government's CheckDoc service www.checkdoc.be) to check if the identity document (ID card, passport, residence permit) is known, genuine and hasn't been revoked.
- the Subject profile is transferred to the C-RA and a certificate and signature service account are created.
- the Subject is provided with information about the service and credential for further authentication purposes.

3) STEP 3 – ENR.AUTH: for subsequent requests (certificate request, signature activation requests), the Subject is authenticated with an **authentication means** that:

i) is unambiguously linked to the person and has been mapped by the SUB-RA and/or the C-RA to that Subject account.

ii) provides a secure mechanism to ensure sole control of the signature key by the Subject

For this purpose, at the time of the registration validation ENR 2, the Subject receives or is associated with a credential that can be used to authenticate the Subject unambiguously toward the Signature Creation Service, and / or to provide a verifiable association between the Subject's request and the previously recorded identity data and attributes of the Subject.

Authentication of additional Attributes for Subjects

In some cases, the CA may also certify professional attributes or membership attributes in addition to identity. The validation of these attributes is the responsibility of the Subscriber and the burden of proof falls upon the Subject and the Subscriber.

The Subscriber may attest to a Subject's professional attribute such as an official degree, a diploma, a mandate, etc., as specified in the applicable Subscriber's agreement.

The Subscriber may attest to a Subject's membership of or relationship with the organisation it represents such as member, employee, associate, role, department, customer, etc.

The Subscriber cannot attest any relationship between a Subject and a third-party organisation.

3.2.4 Non-verified Subscriber information

No stipulations.

3.2.5 Validation of authority

Organisations as Subscriber defines and controls which Subjects are entitled to a certificate. The definition of the validation of authority may be detailed in the Subscriber Agreement. See also section 3.2.3.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-key requests are certificate requests for replacing an existing certificate and key with a new certificate and new key for the same Subject. Rekey requests are typically treated as new certificate requests (see section 3.2.2 and 3.2.3) or alternatively may be processed based on the authentication credential provided in STEP 3 ENR.AUTH described in 3.2.3 above. However, if documents or attestations for the proof of identity used in STEP 2 REG 2 have expired since the previous registration procedure, then the applicant may be asked to present a valid replacement or equivalent.

3.3.2 Identification and authentication for re-key after revocation

Re-key requests are processed as new certificate requests. Before such new certificates are issued, the identity and attributes of the Subject will be verified as described in section 3.2.2 and 3.2.3 .

If documents or attestations for the proof of identity have expired since the previous registration procedure, then the applicant must present a valid replacement or equivalent.

3.4 Identification and authentication for revocation request

Revocation requests can originate from the CA, the Subscriber or the Subject.

Unless the Subject Agreement informs the Subject otherwise, he requests revocation through the Subscriber. The Subscriber authenticates the Subject.

The revocation request can be in the form of a signed document by the Subject and/or the revocation can be in the form of a request which is sent by the Subscriber to the SRA through an authenticated channel.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Only natural persons registered as per 3.2.3 can request a certificate. The Subject must comply with the provisions and obligations set forth in the registration form, in the applicable Subject Agreement, this CP and the Certificate 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 various entities that are collectively referred to as the Registration Authority or RA under the responsibility of ZETESCONFIDENS. For a description of these entities and their respective roles and relationship, please see section 1.3.2.

Regardless of the arrangement, ZETESCONFIDENS assumes final responsibility and accountability for the functioning of the Registration Authority as a collective entity.

ZETESCONFIDENS provides the infrastructure and the operational resources for the Central RA. The Central RA relies on the enrolment process performed by the Subordinate RAs. The Subordinate RAs may delegate the enrolment process to their Local RAs.

The Subordinate RA, and where relevant the Local RA, is responsible for verifying:

- the claimed identity of the applicant,
- the claimed attributes of the applicant,
- the applicant's entitlement to the requested certificate(s),
- the association of an authentication means with the applicant,

This enrolment process is done in accordance with the rules and methods described in this document, the RA Agreement and in the internal guidelines and rules of the RA entities. Each RA entity must archive the received or added information for each certificate request or revocation request. The archive must be kept in a secure location or on a secure system.

4.1.2.2 The Subject Enrolment Process

See also section 3.2.3.

The Subordinate RA collects the required documents and attestations for the subsequent validation of the applicant's identity and attributes. The L-RA or SUB-RA does a first check of the presented documents and attestations and makes sure that the collected information is complete and correct. The L-RA or SUB-RA also informs the applicant about his/her rights and obligations.

The enrolment process may be implemented as a face to face registration process in person or online (video interview), a web form or a by means of an electronically signed enrolment document. In any case, the RA will ensure that the assurance level of the enrolment process complies with the requirements for the ETSI standardized certificate policy for respectively LCP or NCP+, and with the requirements for assurance level "substantial" or "high" as defined in Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

The Subordinate RA is responsible for providing and/or checking information regarding the applicant's attributes (professional attributes, organisational attributes, etc.), if any. The subordinate RA completes the enrolment data if necessary.

The Subordinate RA is responsible for the correct registration/enrolment of Subjects and for supplying the Central RA with the correct data and the Subject's attributes (in particular the accuracy of the data that will be incorporated in the certificate and of the data associated with the authentication means associated with the Subject (e.g. the mobile phone)). The Subordinate RA may delegate these tasks to the Local RAs and may rely on the Local RA for maintaining the registers with the Subject's attributes.

The Central RA (C-RA) is responsible for the correct authentication of the Subscriber and has final responsibility for the correct registration/enrolment of Subjects. The Central RA performs a final technical validity check on the data supplied by the SUB-RA.

4.1.2.3 The Subject Agreement

With the invitation to proceed in the enrolment or at registration, the Subject is supplied with the following information:

- the registration form including the privacy statement
- reference where to download the present CPS, the Signing Service Practice Statement [ref. 5] the TSPS [ref. 4] and the CTC [ref. 3]
- (the case being) bylaws, notices or other documents provided by the Subscriber
- (where an external organisation other than the Subscriber supports the TSP in its RA role) information on the applicable policies and practices

The Subject Agreement needs to be ratified by the subject at the latest when accepting the certificate(s). This is considered the formal acceptance by the Subject of the Subject Agreement whereby the Subject accepts

- responsibility that the information provided by the Subject to the RA is correct, complete, valid and up to date,
- that the Subordinate RA and/or ZETESCONFIDENS maintain 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) or the Subordinate RA ceases its activities, this data may be transferred to a third party, respecting the same terms and conditions as defined in the Subject Agreement,
- acknowledges the rights, obligations and responsibilities of ZETESCONFIDENS and the other PKI Actors, as defined in the Subject Agreement and by law,
- the Subject 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 (i.e. a certificate for signature services compliant with the ETSI policy of resp. LCP or NCP+), with a certain content (i.e. the set of Subject's attributes provided at the registration steps that will be certified).

4.1.2.4 Enrolment of Subscribers

Subscribers are not enrolled. ZETESCONFIDENS enters into a Subscriber Agreement with Subscribers. but does not enrol Subscribers.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Request for Subject's certificate originates from the related Subscriber's SUB-RA. The SUB-RA is authorized by the C-RA according to means stipulated in the Subscriber's agreement.

4.2.2 Approval or rejection of certificate applications

The Central RA 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 of for other reasons, at the discretion of and under the responsibility of ZETESCONFIDENS.

Certificate requests are passed from the C-RA to the Signature Creation Services that generates a private key and formally formats the certificate request for 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.

The C-RA exchanges with the Signature Creation Service and with the CA:

1. the information to be certified related to the Subject, as registered (see 1.3. , 3.2. and 4.1.2)
2. the information related to the type of certificate (i.e. LCP or NCP+)
3. authentication information for subsequent signature operations

4.2.3 Time to process certificate applications

No stipulations.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA and the Signature Creation Service are integrated systems internal to ZETESCONFIDENS. The CA will only process requests that originate from the Signature Creation Service RA module., which is a trusted system internal to ZETESCONFIDENS.

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

- The CA will check that the request originates from Signature Creation Service RA module
- The CA will check the requester's authorization for the type of request and refuse requests that pertain to certificate profiles for which the requester is not authorized.
- The CA also 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 Subject is implicitly notified when the Subscriber' grants the Subject access to the documents to be signed on the Signature Creation Service document platform.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate is accepted by the Subject upon the Subject's declaration of acceptance of the Subject Agreement and the Subject's first use of the certificate through the ZETESCONFIDENS Signature Creation Service.

The Subject must reject the certificate before first use if one or more of the following conditions is true:

- the information in the certificate is incorrect, incomplete or is no longer valid,

- the Subject is no longer entitled to the certificate,
- the Subject does not wish to accept the certificate
- the Subject refutes its relationship with the Subscriber.

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 Subject private keys and related certificates are used for the purposes described in section 1.4. The Subject can only use their keys and certificates through the ZETESCONFIDENS Signature Creation Service.

The Signature Creation Service ensures that:

- the private key cannot be extracted from the QSCD
- the private key is under the (sole) control of the Subject by means of the authentication mechanism mapped to the Subject at the registration Step 3. ENR.AUTH.

The Subject is bound by the usage conditions and obligations mentioned in the Subject 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.

Further details are provided in the Signing Service Practice Statement [Ref. 5].

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

The CA does not renew existing certificates for existing keys. ZETESCONFIDENS reserves the right to enhance the policy in the future to introduce certificate renewal.

4.7 Certificate re-key

The CA may issue a new certificate for a new key for a previously registered Subject. Subject name and identifiers in the certificate are derived from the preceding certificate or from the original registration data.

4.8 Certificate modification

The CA does not issue modified certificates to replace existing certificates for existing keys. ZETESCONFIDENS reserves the right to enhance the policy in the future to introduce certificate modification.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Under normal circumstances revocation is applied:

- If the Subject 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 no longer represents the Subject,
- If the Subscriber decides that the Subject is no longer entitled to the certificate,
- the private key was compromised,
- in case of a court order,
- 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 Subscriber can request revocation for reasons internal to the Subscriber or on demand of the Subject.

The Subject can exercise its right to demand revocation at will.

Revocation requests by the Subscriber or the Subject must be submitted through the appropriate channels as defined below and in respectively the Subscriber Agreement and the Subject Agreement.

4.9.3 Procedure for revocation request

Revocation requests are submitted to the SRA. A Subscriber may request revocation upon its own initiative or upon explicit request of the Subject. A certificate revocation request triggers the destruction of the Subject's account on the Signature Creation Service which includes the decommissioning of the Subject's private key.

4.9.4 Revocation request grace period for the Subscriber/Subject

A Subscriber or Subject 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 within 24 hours following receipt of the request by the SRA.

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

The CRLs are issued at pre-defined intervals or ad hoc when deemed necessary. The CRL/delta-CRL is refreshed at least every 24 hours. See the CRL profile in section 7.3.

4.9.8 Maximum latency for CRLs

The CRL is available for download within 20 minutes of creation.

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.

4.10 Certificate status services

4.10.1 Operational characteristics

ZETESCONFIDENS provides Certificate Revocation Lists and Online Certificate Status Protocol services for checking the status of the certificates:

CRL and delta-CRL download service

CRLs and delta -CRLs are published at regular intervals on the CRL distribution point (see the Certificate Policy and certificate profile for the certificate). CRLs or delta-CRLs may be renewed ad hoc; e.g. when certificates have been revoked. CRLs or delta-CRLs shall be renewed before the CRL or delta-CRL is about to expire.

OCSP service

The OCSP service is available for unsigned requests via 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. For the OCSP profiles, see section 7.3.

Retention period for Certificate Status Information after expiration of the certificates

Certificate status information in CRLs and through the OCSP service shall be updated at least until all certificates that were issued by the respective CA have either expired or have been revoked. CRLs will contain certificate status information for qualified certificates also beyond the expiration date of the certificate.

4.10.2 Service availability

CRL repository availability shall exceed 99.0% of business hours - defined as 24 hours per day, seven days per week, excluding planned maintenance periods.

OCSP service availability shall exceed 99.5% of business hours - defined as 24 hours per day, seven days per week, excluding planned maintenance periods.

Planned maintenance periods that cause an interruption of service will be announced on http://confidens.zetes.com at least 24 hours in advance.

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.

ZETESCONFIDENS will continue to provide certificate status information to the Subscriber, Subjects and Relying Parties for as long as contractually and legally required.

4.12 Key escrow and recovery

The keys are generated and stored on a QSCD. The intended usage is electronic signature with non-repudiation. Key escrow and key recovery are not supported.

4.12.1 Key escrow and recovery policy and practice

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

See 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.

6 TECHNICAL SECURITY CONTROLS

This section covers the technical security controls for the end entity key pair. 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

The key pairs for Subjects are generated on the QSCD. The key generation process is performed and controlled by the ZETESCONFIDENS Signature Creation Service, see [ref. 5] and according to the registration and procedures described in section 3.2. Only the public part of the key pair can be extracted in clear from the QSCD, for the purpose of creating the associated certificate. The private part of the key pair cannot be exported or extracted in clear but can be backed up in encrypted form.

See [ref. 5] for more details.

6.1.2 Private key delivery to the Subject

The key remains within the ZETES Signature Creation Service environment. Private key delivery is implicit and coincides with the activation of the Subject's account in the Signature Creation Service environment and the provisioning of the Activation Data to the Subject.

See [ref. 5] for more details.

6.1.3 Public key delivery to certificate issuer

The Subject's public key is de facto in possession of the certificate issuer since it is generated by ZETESCONFIDENS Signature Creation Service. The public key is delivered to the certificate issuer through a secure channel within the ZETESCONFIDENS infrastructure.

6.1.4 CA public key delivery to Relying Parties

The ZETESCONFIDENS CA certificates shall be published on https://repository.confidens.zetes.com.

Relying Parties shall be able to authenticate the web site by means of the SSL/TLS server authentication certificate which is issued by a public trust CA. The authentic "thumbprint" of the ZETESCONFIDENS CA certificates shall be published in a document in PDF/A format.

Relying parties may contact ZETESCONFIDENS via e-mail at info@confidens.zetes.com to receive confirmation of the authentic "thumbprint" of the CA certificates by means of an out-of-band channel such as a telephone call, e-mail or letter.

6.1.5 Key sizes

Subject keys for electronic signature are RSA2048 SHA256-with-RSA. ZETESCONFIDENS is not in any way held to continue using the current algorithms, protocols or key lengths should ZETESCONFIDENS decide that the current algorithms, protocols or key lengths provide insufficient assurance and security for the intended purpose and the intended use period.

6.1.6 Public key parameters generation and quality checking

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. Key generation uses hardware supporting FIPS 186-2 RNG. The RSA keys 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. See section 7.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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 30 paragraph 3 lit. B.

Designation of the QSCD:	Qualified Signature and Seal Creation Device (QSCD) Cryptomathic Signer, version 4.8
Manufacturer:	Cryptomathic A/S, Jaegergårdsgade 118, 8000 Aarhus C, Denmark
Certification body:	Zentrum für sichere Informationstechnologie (Austria) www.a-sit.at
Certificate issued on:	2018-07-03
Reference number:	A-SIT-VIG-18-043

The QSCD is Cryptomathic Signer version 4.8 in combination with HSM devices Thales/nCipher nShield Connect/Connect+/Connect XC2 as cryptographic modules for the generation and protection of the signature resp. seal creation data (SCD). The HSMs are operated in strict FIPS 140-2 level 3 mode in conjunction with the published security policies. The HSMs provide a secure protection mechanism “Security World” for storing private keys outside of the HSM in a database. The Signature Activation Module (SAM) is a software module to ensure that users (i.e. signatories or creators of a seal) retain control of their signing keys. It is loaded onto the HSMs as a local application. The QSCD is operated in a secure environment.

For more information, see the Signature Creation Service Practice Statement [ref. 5].

6.2.2 Private key multi-person control

Not applicable for the Subject Private Key.

6.2.3 Private key escrow / backup / archival

Private keys are not put in escrow.

Private keys are not archived.

Private keys cannot be extracted in non-encrypted format from the HSM 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

Private keys are always encrypted (for export operation) or decrypted (for import operation) inside the HSM itself. The encryption key is split over a set of m HSM backup cards. A restore operation requires a pre-defined quorum

of n-of-m HSM backup cards. Each card has an activation code which is independent from the other cards. The cards and the activation data are assigned to individual custodians and are stored in separate locations.

6.2.4 Private key transfer into or from a cryptographic module

Private keys on a QSCD are generated on-board the QSCD's HSM and can be transferred to another QSCD HSM. Transfer of private keys between HSM requires multi-person control in the form of a quorum of *n-of-m* HSM cards.

6.2.5 Private key storage on cryptographic module

Private keys are generated in and stored in a QSCD HSM. See the Signing Service Practice Statement [ref. 5].

6.2.6 Method for activating private keys

The Subject activates its private key in an authenticated session with the ZETESCONFIDENS Signature Creation Service. The authentication means have been securely and unambiguously associated to the Subject at the occasion of the Registration Step 3 ENR.AUTRH. (see sections 3.2 and 4.1.2). The activation of the key is linked to the data-to-be signed through methods described in the Signature Creation Service Practice Statement [ref. 5].

6.2.7 Method of deactivating private key

In the case where the Subscriber can deactivate the authentication means that have been associated to the Subject at the occasion of the Registration Step 3 ENR.AUTRH, the use of the private key itself is also no longer possible. Where the use of the private key is programmed to be used only once after activation, it is automatically deactivated after it is used or if was not used as the next action after the activation process.

See the Signature Creation Service Practice Statement [ref. 5].

6.2.8 Method of destroying private key

The private key can be disabled, decommissioned (irreversibly disabled) or deleted by authorised team of the ZETES Signature Creation Service.

See the Signing Service Practice Statement [ref. 5].

6.2.9 Capabilities and Rating of the Cryptographic Module

Cryptomathic Signer supports the following HSM types for the QSCD:

- Thales/nCipher nShield Connect , Firmware: 2.55.1, 2.61.2
- Thales/nCipher nShield Connect +, Firmware: 2.55.1, 2.61.2
- Thales/nCipher nShield Connect XC, Firmware: 3.4.1

For firmware 2.55.1, the certificate No. 1/1616 – issued on 2016-03-10 by the Italian Common Criteria certification body OCSI applies. The certificate confirms that the HSM was successfully evaluated against Common Criteria version 3.1., Evaluation Assurance Level EAL4+ augmented with AVA_VAN.51.

For firmware 2.61.2 resp. 3.4.1 the following NIST FIPS 140-2 certificates apply:

- FIPS Validation Certificate No. 264018 - issued on 2016-05-13 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body; for Thales – nShield Solo or nShield Connect, firmware version 2.61.2
- FIPS Validation Certificate No. 264419 - issued on 2016-05-13 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body; for Thales – nShield Solo+ or nShield Connect+, firmware version 2.61.2

- FIPS Validation Certificate No. 294120 - issued on 2017-06-23 and last updated on 2017- 11-07 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body; for Thales – nShield Solo XC or nShield Connect XC, firmware versions 3.3.21 and 3.4.1

These certificates confirm that the HSMs were successfully evaluated against FIPS 140-2 level 3.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are archived in the form of the certificates that contain the public key.

6.3.2 Certificate operational periods and key pair usage periods

No stipulations.

6.4 Activation data

A Subject must first be registered by a Registration Authority (RA). To access the application and the subsequent signing and seal creation service, the user also needs to login using the credentials defined in the registration process. Some or all authentication factors are verified by an external identity provider (IdP) that will issue a SAML Assertion. If all the credentials are verified by the IdP these must correspond to an authentication means equivalent to Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 for assurance level substantial or higher . If only some of the credentials are verified by the IdP and these are not enough to correspond to an authentication means equivalent to Commission Implementing Regulation (EU) 2015/1502 for assurance level substantial or higher, an additional factor is required to trigger the seal or signing operation. This factor may be one of the following supported token-types: OATH-TOTP, OATH-HOTP, OATH-OCRA, SMS, Belgian Mobile itsme®, FIDO token or other additional factor. The SAML assertion is send to the SAM, which verifies the assertion.

6.5 Computer security controls

ZETESCONFIDENS ensures computer security controls described in the TSPS [ref. 4].

6.6 Life cycle technical controls

ZETESCONFIDENS ensures life cycle technical controls described in the TSPS [ref. 4].

6.7 Network security controls

ZETESCONFIDENS ensures network security controls described in the TSPS [ref. 4].

6.8 Time-stamping

ZETESCONFIDENS ensures UTC-synchronisation controls described in the TSPS [ref. 4].

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.

7.1.1 The ZETESCONFIDENS 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**
Subject serialNumber = 001
certificate serial number = 38 20 EE 9C 74 EC D1 47
SHA1 thumbprint = 16 98 DC 47 F4 F5 FF 95 6C 56 03 24 E1 96 5A A7 ED 38 E2 9D

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 Signature for natural persons

This certificate profile is for certificates issued in accordance with the LCP and NCP+ Certificate Policy and complies with the corresponding certificate profiles defined in ETSI EN 319 412-1/2 for a natural person (the Subject) with a key pair generated, stored and managed on a remote Secure Cryptographic Device managed by the ZETESCONFIDENS Signature Creation Service.

Table 1 Certificate profile for natural persons (LCP/NCP+)

Certificate profile conforming to ETSI LCP and NCP+ version 1.1			
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	**serialNumber**	-	variable, mandatory, ETSI TS 319 412 part 2
	givenName	-	variable, mandatory, ETSI TS 319 412 part 2
	surname	-	variable, mandatory, ETSI TS 319 412 part 2
	commonName	-	variable, mandatory, ETSI TS 319 412 part 2
	countryName	-	variable, mandatory, ETSI TS 319 412 part 2
	title	-	variable, optional
	emailAddress	-	variable, optional
	organizationName	-	variable, optional
	organizationIdentifier	-	variable, optional, ETSI TS 319 412 part 1 and part 2
	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**	-	Id-ad-1 **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	-	Id-ad-1 **OID 1.3.6.1.5.5.7.48.1** {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**
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 v2.1.1 chapter 4.3.2 key usage type A
certificatePolicies	**policyIdentifier**	-	ZETESCONFIDENS Policy Identifier: OID = **1.3.6.1.4.1.47718.2.1.2.2.4.1** for LCP OID = **1.3.6.1.4.1.47718.2.1.2.2.4.2** for NCP+
	policyIdentifier	-	ETSI Policy Identifier: OID = **0.4.0.2042.1.2** for NCP+ OID = **0.4.0.2042.1.3** for LCP

	policyQualifierId	-	Id-qt-1 (**CPS**)
	Qualifier	-	**https://repository.confidens.zetes.com/**
basicConstraints	**subjectType**	c	**False** (CA = false)

7.1.3 Certificate Profile for Qualified Electronic Signature for natural persons

This certificate profile is for certificates issued in accordance with the QCP-n-qscd Certificate Policy and complies with the corresponding certificate profiles defined in ETSI EN 319 412-1/2/5 for a natural person (the Subject) with a key pair generated, stored and managed on a remote QSCD managed by the ZETESCONFIDENS Signature Creation Service.

Table 2 Certificate profile for natural persons (QCP-n-qscd)

Certificate profile conforming to ETSI QCP-n-qscd version 1.1			
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	**serialNumber**	-	variable, mandatory, ETSI TS 319 412 part 2
	givenName	-	variable, mandatory, ETSI TS 319 412 part 2
	Surname	-	variable, mandatory, ETSI TS 319 412 part 2
	commonName	-	variable, mandatory, ETSI TS 319 412 part 2
	countryName	-	variable, mandatory, ETSI TS 319 412 part 2
	title	-	variable, optional
	emailAddress	-	variable, optional
	organizationName	-	variable, optional
	organizationIdentifier	-	variable, optional, ETSI TS 319 412 part 1 and part 2
	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**	-	Id-ad-1 **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	-	Id-ad-1 **OID 1.3.6.1.5.5.7.48.1** {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**
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 v2.1.1 chapter 4.3.2 key usage type A
certificatePolicies	**policyIdentifier**	-	
	policyIdentifier	-	ZETESCONFIDENS Policy Identifier: OID = **1.3.6.1.4.1.47718.2.1.2.2.4 .3** for QCP-n-qscd
	policyIdentifier	-	ETSI Policy Identifier: OID = **0.4.0.194112.1.2** for QCP-n-qscd
	policyQualifierId	-	Id-qt-1 (**CPS**)

	Qualifier	-	**https://repository.confidens.zetes.com/**
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: 0.4.0.1862.1.6.1** {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcType(6) qct-esign(1)}
	qcSSCD	-	**OID: 0.4.0.1862.1.4** {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) QcSSCD(4)}
QcPDS	**PdsLocations**	-	**OPTIONAL** **OID: 0.4.0.1862.1.5** sequence of 1 or more sets of language code + URL for the PKI Disclosure Statement (PDS)
	url	-	**https://pds.confidens.zetes.com**
	language	-	ISO 639-1 language code **EN**

7.1.4 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 shall clearly indicate that these are for testing purposes (a.o. in the subject name, organization name, the proprietary policy OID, the user notice statement, etc.):

- **subject serial number** is the same format as for real certificates, but all digits are set to zero
- **subject givenName** is“givenName_TEST”
- **subject surName** is“surName_TEST_xxxxxx” where xxxxxx is a 6-digit number
- the name components of the **subject commonName** are “surname_TEST_xxxxxx givenName_TEST” with prefixes and suffixes as in the real certificate
- if an e-mail address is used for **emailAddress** or in the subject alternate name, then it must be an e-mail address for test purposes, i.e. not the e-mail address of a genuine Subject
- **subject Organization and OrganizationalUnit** are prefixed with “TEST “
- 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

  This URL remains identical as those in the real certificates because the certificate must point to the real CP/CPS which also contain the information about the test certificates.
- **generic policy identifiers (OID)**:
  No differences, to allow testing whether 3rd party application correctly interpret and display these standardized generic OIDs
- **proprietary policy identifiers (OID):**
  Proprietary OID are pre-fixed with the value “2.999.”.

** Remark: 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 real 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.*

7.2 OCSP certificate profile

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

7.3 CRL profile

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The ZETESCONFIDENS Trust Services Practice Statement [ref. 5] 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. 5] applies.

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

The Subscriber/Subject Agreement also contains the Certificate Terms and Conditions for the use of the Certificates under this CP, which have been provided to the Subject before acceptance and are accepted by the Subject as part of its Subject Agreement.

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----------