ZETES TSP QUALIFIED CA 001

CERTIFICATE POLICY FOR OVB-OBFG-OAC

Certificate Policy

for certificates issued on behalf of

OVB-OBFG-OAC

Publication date :	**05/03/2021**	
Effective date :	**08/03/2021**	
Document OID :	**1.3.6.1.4.1.47718.2.1.2.2.1.10 (NCP+)** **1.3.6.1.4.1.47718.2.1.2.2.3.10 (QCP-n-qscd)**	
Version :	**1.8**	**02/03/2021**

Table of Content

Tables

ABOUT THIS DOCUMENT

Scope

The present document is a Certificate Policy (CP) for certificates issued by the ZETES TSP Qualified CA 001.

The policy applies to the issuance of Normalized Certificates meeting the requirements of ETSI EN 319 411-1 **[ref. 2]** and of Qualified Certificates meeting the requirements of Regulation (EU) No 910/2014 **[ref. 1]** and 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
1.8	05/03/2021	xx/03/2021	Including reference to TSPS for identity validation methods.
1.7	02/10/2020	05/10/2020	NCP+ certificate profile: added information regarding the new URL (confidens.zetes.com instead of tsp.zetes.com), the use of ECC384 and the "CERT" prefix in the Subject CN.
1.6	03/09/2020	04/09/2020	NCP+ certificate profile additional EKU for e-mail signing and change of User Notice text. Update of references. Inclusion of online registration and validation method. 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.
1.5	09/09/2019	12/09/2019	Clarifications regarding CommonName
1.4	11/09/2018	14/09/2018	Clarifications regarding key & certificate lifecycle.
1.3	11/06/2018	13/06/2018	Adding the OAC (Bar for lawyers at the Cour de cassation) to the subscriber, updating Certificate Profile options. --------
1.2	17/07/2017	21/07/2017	Additional clarifications and information, in alignment with the relevant CPS. Changes in the certificate profiles and information about test certificates. --------
1.1	17/05/2017	22/05/2017	Harmonisation with CPS v1.2. Adaptation of the registration procedure for Subjects (deleted possibility to register via mail or fax). --------------------
1.0	27/03/2017	29/03/2017	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) (OID 1.3.6.1.4.1.47718.2.0.1.1)

[ref. 5] ZETES TSP QUALIFIED CA 001 - Certification Practice Statement (CPS)

ABOUT ZETES

General information about Zetes SA can be found in the TSPS [ref. 4].

1 INTRODUCTION

1.1 Overview

The OVB-OBFG-OAC Certificate Policy (CP)

This Certificate Policy specifically applies to the certificates issued by the ZETES TSP Qualified CA on behalf of the following three organisations:

- **OVB** – *"Orde van Vlaamse Balies",* composed of the Belgian (Dutch speaking) local Bar Associations as defined in Article 488 of the Belgian Judicial Code
- **OBFG** – *"l'Ordre des Barreaux Francophones et Germanophone de Belgique"*, composed of the Belgian (French and German speaking) local Bar Associations as defined in Article 488 of the Belgian Judicial Code
- **OAC** – *"Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie"*, being the Bar Association as defined in Article 481 of the Belgian Judicial Code

These organisations are collectively referred to as OVB-OBFG-OAC and are considered as a single entity when seen as the Subscriber for the certificates under this policy. They may be referred to separately as OVB, OBFG and/or OAC when seen in their respective role as organisation fulfilling tasks such as Subordinate Registration Authority (SUB-RA).

The provision and use of (Qualified) Certificates issued by ZETES TSP Qualified CA are governed by the following documents:

- the ZETES TSP QUALIFIED CA 001 - Certification Practice Statement (CPS) **[ref. 5]**,
- the present Certificate Policy (CP),
- the applicable Certificate Terms and Conditions (CTC).

The present document states the policies applicable to certificates issued for OVB, OBFG and OAC in terms of certificate profiles, applicability and management lifecycles. It defines the procedures for Subject enrolment, certificates issuance, revocation etc.

Every certificate contains a Certificate Policy OID corresponding to the type and the assurance level of the Certificate. Every certificates is complemented by an OID identifying its domain of issuance and authorised Subscriber.

Policy	Policy Identifiers	Description
NCP+	**0.4.0.2042.1.2**	Policy conforming to ETSI EN 319 411-1 for an Enhanced Normalized Certificate issued to natural persons requiring a Secure Cryptographic Device based for the support of a wide variety of application including but not limited to authentication of the certificate holder.
	1.3.6.1.4.1.47718.2.1.2.2.1.10	ZETES TSP NCP+ certificate for natural persons for the Subscriber OVB-OBFG-OAC.
QCP-n-qscd	**0.4.0.194112.1.2**	Policy conforming to ETSI EN 319 411-2 for a EU Qualified Certificate issued to natural persons requiring a Qualified Signature Creation Device for the support of Qualified Electronic Signature based on a qualified certificate defined in articles 3 (12) and 28 of the Regulation (EU) No 910/2014.
	1.3.6.1.4.1.47718.2.1.2.2.3.10	ZETES TSP QCP-n-qscd certificate for natural persons for the Subscriber OVB-OBFG-OAC.

Conformity with RFC 3647

The present CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 framework and template for Certificate Policy and Certification Practice Statement construction.

It contains information pertaining to end-entities certificates' profiles, applicability and management lifecycles. The CA practices, including amongst other, the PKI (CA and related components) certificate profiles, applicability and management lifecycles are to be found in the CPS.

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

This CP is in accordance with the requirements laid down in the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. In particular, it respects requirements for Qualified Trust Services Provider (QTSP) and for Qualified Certificates where applicable.

This CP conforms to the requirements laid down in ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements" and ETSI EN 319 411-2 "Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing Qualified Certificates" where applicable.

Non-disclosure

For reasons of confidentiality, ZETES cannot disclose all details on controls in this CP, 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 section 5.2 of the ETSI EN 319 411-2 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 Common Certificate Policy for OVB-OBFG-OAC'. It covers the certificates policies for NCP+ certificate and QCP-n-qscd certificates and is therefore identified by two Certificate Policy OIDs.

In particular, the present Certificate Policy document covers the following certificate policies:

ZETES TSP Qualified CA - NCP+ certificates for OVB-OBFG-OAC	
dotted notation	1.3.6.1.4.1.47718.2.1.2.2.1.10
full notation	{ iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) zetes(47718) zetes-tsp(2) cs(1) cert-policy(2) qca(2) ncp+(1) ovb-obfg-oac(10)}

ZETES TSP Qualified CA - QCP-n-qscd certificates for OVB-OBFG-OAC	
dotted notation	1.3.6.1.4.1.47718.2.1.2.2.3.10
full notation	{ iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) zetes(47718) zetes-tsp(2) cs(1) cert-policy(2) qca(2) qcp-n-qscd(3) ovb-obfg-oac(10)}

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 ZETES TSP as a Certification Services Provider (CSP) and/or who are impacted by the use of certificates issued by ZETES TSP acting as a CSP. All participants adhere to or are bound by the Certification

Practice Statements and Certificate Policies that are maintained by ZETES TSP. The PKI participants involved in any of the processes and activities of ZETES TSP as a CSP are also called PKI Actors.

For the context of this Certificate Policy, the PKI participants are defined as follows:

Subscriber	The Subscriber enters into a contractual agreement with ZETES TSP on behalf of the Subjects. For this CP, the Subscriber is the OVB-OBFG-OAC.
Subjects	Natural persons whose identity or identifier is encoded in the end user certificate issued by a CA. A Subject adheres to a Subscriber. For this CP, the Subject is a lawyer who is a registered member of OVB, OBFG or OAC, or a registered staff member associated with a lawyer's office.
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. For this CP, the CA is the Zetes TSP Qualified CA.
CSP - Certificate Service Provider	The entity that has final and overall responsibility for the provision of the (Qualified) Certificates. For this CP, the CSP is ZETES TSP .
RA - Registration Authority	The entity representing the overall organisation of registration authority bodies. The RA as supervising authority over the C-RA, SUB-RA and L-RA, authenticates registration/certificate requests from the SUB-RA.
C-RA - Central Registration Authorities	The central infrastructure hosted by ZETES TSP. It handles the registration and vetting of certificate requests received from the SUB-RAs. The C-RA coordinates the certificate creation process between the Secure Cryptographic Device/card personalisation services and the CA. It is the only part of the RA that is in direct contact with the CA or with the card personalisation infrastructure.
SUB-RA - Subordinate Registration Authorities	The SUB-RA is the authority for the registration and vetting of Subjects and certificate requests for a specific Subscriber or group of Subscribers. The SUB-RA is usually associated with or part of the Subscriber. For this CP, the SUB-RAs are the OVB, OBFG and OAC.
L-RA - Local Registration Authorities	The L-RA is the local representative of the SUB-RA. The L-RA performs the front-office registration tasks and first-line vetting of Subjects. For this CP, the task of L-RA is performed by the local bar associations (NL "*balies" / FR "barreaux"*) for OVB and OBFG. OAC may have one or more L-RA.

SRA - Suspension and Revocation Authority	ZETES TSP 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	Online publication of documents such as Certification Practice Statements, Certificate Policies, TSP terms and conditions, certificate validation data such as root certificates, certificate revocation lists, etc.
Secure Cryptographic Device - Provisioning Services	ZETES TSP is responsible for supplying the Secure Cryptographic Device.
Secure Cryptographic Device - Personalisation and Delivery Services	These are the smartcard personalisation services by Zetes, i.e. the process of printing the card body, encoding the chip and generating the cryptographic keys on the chip, printing the PIN/PUK letter, etc. Card Delivery Services by Zetes i.e. the process of distributing the cards and PIN/PUK letters to the Subjects.

Any further reference to Registration Authority entities in the present document implicitly also refers to the equivalent Suspension & Revocation Authority entities.

1.3.1 Certification Authority

ZETES TSP Qualified CA is responsible for:

- Issuing Normalized Certificates and Qualified Certificates to Subject on request of the C-RA;
- Issuing CRLs (Certificate Revocation List) on a regular basis or when a certificate status change occurs;
- Providing OCSP (On-line Certificate Status Protocol) services

For more information, see the ZETES TSP QUALIFIED CA 001 - Certification Practice Statement (CPS) **[ref. 5]**.

1.3.2 Registration Authority (RA)

1.3.2.1 Overview

The Registration Authority is the entity that is responsible for:

- Authenticating and vetting certificate requests and revocation requests;
- Applying the naming conventions defined within this document when creating new entities, so that each entity is uniquely and unambiguously identified;
- Requesting the CAs to produce the certificates for approved certificate application requests;
- The certificate delivery Service
- Requesting the CAs to revoke the certificates for approved revocation application requests;
- 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 information that it stores and processes is handled in a manner that is consistent both with the policies and procedures defined in this document and with the ZETES security's regulations.

The RA is organised as a multi-tier organisation. The operational tasks of the RA are performed by the Central Registration Authority, one or more Subordinate Registration Authorities and their Local Registration Authorities.

The operational aspects of the RA are detailed in the CPS **[ref. 5]**.

1.3.2.2 Central Registration Authority (C-RA)

The Central RA is the organisational structure and the infrastructure of the RA within ZETES TSP.

For more information, see the ZETES TSP QUALIFIED CA 001 - Certification Practice Statement (CPS) **[ref. 5]**.

1.3.2.3 Subordinate Registration Authorities (SUB-RA)

In the case of the present CP, OVB, OBFG and OAC are the Subordinate Registration Authorities. They organise and coordinate the registration and certificate delivery to lawyers and to staff members. For this purpose, OVB and OBFG delegate the actual registration process to their respective local Bar Associations, which fulfil the role of the Local Registration Authorities. OAC may delegate the actual registration process to one or more centrally organised office, which fulfils also the role of the Local Registration Authority.

1.3.2.4 Local Registration Authorities (L-RA)

In the case of the present CP, the local Bar Associations of respectively OVB and OBFG are performing the role of Local RAs and are responsible for the actual registration of the lawyers/staff members for whom the certificates are intended. For OAC there is one or more centrally organised office, which fulfils the role of the Local Registration Authority for its members.

For the OVB - *Orde van Vlaamse Balies* :

- L-RA offices for the Local Bar Associations in the Region of Flanders

- one L-RA office in Brussels at the *Nederlandse Orde van Advocaten bij de Balie te Brussel*

For the OBFG - *Ordre des Barreaux Francophones et Germanophone de Belgique* :

- L-RA offices for the Local Bar Associations in the Region of Wallonia
- one L-RA office in Brussels at the *l'Ordre français des avocats du barreau de Bruxelles*

For the OAC – *"Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie"* :

- one L-RA office in Brussels located at the office of *de Nederlandse Orde van Advocaten bij de Balie te Brussel*
- one L-RA office in Brussels located at the office of *l'Ordre français des avocats du barreau de Bruxelles*

The registration process is described in chapter 3, chapter 4 and in the detailed underlying procedures provided in confidential documents that are part of the Subscriber agreement.

1.3.3 Subscriber and Subjects

1.3.3.1 Subscriber (organizations)

In the case of the present CP, OVB-OBFG-OAC is the Subscriber. These organizations have entered into a Subscriber Agreement with ZETES and they may request issuance, revocation or renewal of end-entity certificates for Subjects under their care, as defined in the Subscriber Agreement. In addition, the CPS, the present CP and CTC are an integral part of the Subscriber Agreement.

The Subscriber is also responsible for:

- Immediately notifying the RA upon (suspicion of) private key compromise;
- Submitting requests for renewal of keys and/or certificates to the RA in due time;
- Notifying Subjects at least one month before a certificate is about to expire.

1.3.3.2 Subjects (natural persons)

In the case of the present Certificate Policy, the Subject can be:

- a lawyer who is a registered member of OVB, OBFG or OAC,
- a staff member of a lawyer's office, who has been registered as such with OVB or OBFG

Subjects must sign a Subject Agreement that complements the Subscriber Agreement that globally rules the issuance of certificate to Subjects represented by the Subscriber. This Subject Agreement refers to the CPS, the present CP, the related CTC and any other element signed by the Subject such as the registration form.

The Subject is the end user of the certificate and is responsible for the proper use of the certificate in compliance with the rules laid down in the Certificate Policy. These responsibilities include proper use of associated equipment (e.g. a smartcard) and associated information (e.g. PIN codes, PUK codes, passwords, revocation validation secrets, etc.).

Subjects may request issuance, suspension, revocation or renewal of end-entity certificates for themselves as defined in the contractual agreements between the Subscriber and Zetes. The terms are reflected in the corresponding Subject Agreement.

A Subject is also responsible for:

- Immediately notifying the RA upon (suspicion of) private key compromise;
- Submitting requests for renewal of keys and certificates to the RA in due time;
- Ensuring that the confidentiality of their private key is protected in a manner that is consistent with this document;

- Ensuring that access to use of their private key is controlled in a manner that is consistent with this document.

1.3.4 Relying parties

The Relying Parties are those parties who are relying on a ZETES TSP (Qualified) 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.

1.3.5 Other participants

1.3.5.1 Secure Cryptographic Device Provisioning Services

The Secure Cryptographic Devices required to contain the private key corresponding with the certified public key are provided by ZETES.

The creation of the key pairs is performed by and under control of ZETES as part of the Secure Cryptographic Device personalisation process. The private key is generated in the Secure Cryptographic Device and cannot be extracted from it.

ZETES has its own department for taking care of transport and registered delivery of the Secure Cryptographic Device to the LRA offices which serve as issuance points.

1.3.5.2 Dissemination and Repository Services

ZETES is responsible for operating the Dissemination Services (publication of Certification Practice Statement, Certificate Policy, 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, Certificate Policy, 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.

1.3.5.3 Revocation Management Services and Revocation Status Information Services

ZETES TSP 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 (Qualified) Certificates that are ruled by the ZETES Qualified (Certificates) Certificate Policy.

1.3.6 ZETES TSP Policy Management Authority (PMA)

The PMA is the high-level management body that has overall responsibility for the TSP Services. The PMA includes senior members of management as well as staff responsible for the operational management of the ZETES TSP PKI environment.

The PMA responsibilities are detailed in the CPS **[ref. 5]**.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

This Certificate Policy covers the issuance of the following types of certificates:

- Certificates for the Authentication of the Subject.
- Certificates for the support of Qualified Electronic Signature based on a Qualified Certificate defined in articles 3 (12) and 28 of the Regulation (EU) No 910/2014.

The certificate use is encoded in the certificate itself, in compliance with the following relevant standards:

- 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 (CRL) Profile (see also chapter 6.1.7)

It is the responsibility of the Subject to use the certificates accordingly. It is the Subject's or the Subscriber's responsibility to use software applications 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, 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 of the certificate.

The appropriate certificate usage is further described (where applicable) in the Certificate Terms and Conditions for the certificate.

1.4.2 Prohibited certificate uses

Any usage of a certificate other than the usage explicitly allowed in the present CP or Certificate Terms and Conditions, is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

The present document is administered by the ZETES TSP Policy Management Authority (PMA).

1.5.2 Contact person

All questions and comments regarding the present document should be addressed to the representative of the Policy Management Authority (PMA):

Contact address:	pma@tsp.zetes.com	
Postal address:	Straatsburgstraat 3 1130 HAREN BELGIË	3, rue de Strasbourg 1130 HAEREN BELGIQUE
Telephone:	0032 2 728 37 11	
Fax:	0032 2 728 37 52	
Web site:	http://tsp.zetes.com	

1.5.3 Person determining suitability for the policy

The PMA determines the present document’s suitability for the ZETES TSP certification services.

1.5.4 CP approval procedures

The PMA is responsible for the approval of the CP. The existing ZETES Change Control mechanism will be used to trace all identified changes to the content of this CP.

This CP shall be reviewed in its entirety every year or when major changes are implemented.

Errors, updates, or suggested changes to this CP shall be communicated to the Policy Management Authority.

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
CSP	Certification Service Provider
CTC	Certificate Terms and Conditions
DN	Distinguished Name
HSM	Hardware Security Module
LRA	Local Registration Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority

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 make reference 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.

Normalized Certificate

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

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 *Certification Practice Statement*, the term Qualified Certificate will only reference to “qualified certificates for electronic signature” under the Regulation.

Relying party

In the context of this *Certification Practice Statement*, Relying Parties are as defined in section 1.3.4.

Subscriber

In the context of this *Certification Practice Statement*, the Subscribers are as defined in section 1.3.3.1.

Secure Cryptographic Device

For the present CP the Secure Cryptographic Device refers to the cryptographic device provided to end-entities (e.g. Subjects). These Secure Cryptographic Devices may come in different form such as e.g. an ID-1 size smartcard, a SIM- size smartcard or a USB device (similar in shape to a USB memory stick), etc.

The Secure Cryptographic Device provides some or all of the following functions:

- generating electronic signatures over previously externally calculated hash values,
- generating keys inside the device
- importing keys into the device
- the device is able to protect the secrecy of the stored private key,
- the device restricts the usage of the key to the authorised Subject only by means of a PIN code or an equivalent authentication mechanism such as biometric Match on Card

For the purpose of a Qualified Electronic Signature (QES) with a certificate that adheres to the policy [QCP-n-qscd], the Secure Cryptographic Device complies with the following requirements for a Qualified Signature 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):

- The Secure Cryptographic Device 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 pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014.
- Specifically, the Secure Cryptographic Device has passed security certification in compliance with ETSI EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation and ETSI EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application.

Note: the term “SSCD” or “Secure Signature Creation Device” is deprecated as of 1st July 2016.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ZETES TSP shall operate services 24/7 for the publication of information for Subscribers, Subjects and Relying Parties.

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

The same information shall also be available for manual download from the ZETES TSP web site. Supporting information such as the various (versions of) Certification Practice Statement documents, Certificate Policy documents, etc. are also available for download from the same web site.

The complete overview of online repositories and services is detailed in the CPS **[ref. 5]**.

2.2 Publication of certification information

Availability

Availability of the document repository is detailed in the CPS **[ref. 5]**.

Publication of Subject/Subscriber certificates in a repository

Taking into account that

- The ZETES TSP Qualified 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,
- All modern protocols and formats for authentication and electronic signature include the Subject's certificate with the signed data and thereby allows the Relying Party to retrieve the certificate from that source,
- Subject certificates for natural persons are securely distributed on the Secure Subject Device / Smartcard of the certificate holder,
- Certificates contain privacy sensitive information,
- The act of publication or retraction of a certificate from a repository may in itself be privacy sensitive,

ZETES TSP, as a matter of policy, does not publish certificates issued to Subjects/Subscribers (end entity certificates) in a public certificate repository. This policy is clearly stated in the contractual agreement with the Subscriber (if applicable).

Relying parties need to consider the fact that end entity certificates will not be published. It is the responsibility of the Subject or Subscriber to include the end entity certificate with the signed data, be it for authentication purposes or signature purposes. It is the responsibility of the Relying Party to extract the certificate from this source and validate the trust chain of the extracted certificate correctly.

Publication of CA certificates in a repository

ZETES TSP publishes its CA certificates in a public certificate repository (http://crt.tsp.zetes.com).

These certificates can be downloaded manually by or automatically by software applications. The fingerprint information for these certificates is stated in the Certification Practice Statement document for the CA.

Relying parties who wish to validate these values before installing the CA certificates, can obtain out-of-band confirmation within 3 working days via

info@tsp.zetes.com

Certificate Status Information

For more information, see section 4.10 and the ZETES TSP QUALIFIED CA 001 - Certification Practice Statement (CPS) **[ref. 5]**.

2.3 Time or frequency of publication

Publication of CA certificates in a repository

New CA Certificates shall be 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 shall be renewed before the CRL or delta-CRL is about to expire and may be renewed at any time when certificates have been revoked. CRLs are updated until all certificates that were issued by the respective CA key have expired.

For more information, see the ZETES TSP QUALIFIED CA 001 - Certification Practice Statement (CPS) **[ref. 5]**.

Publication of terms and conditions, certificate policies, etc.

Updates to the Certificate Policy, Certification Practice Statement, TSP terms and conditions, and other public documents shall be published whenever a change occurs, ensuring a period of minimum two (2) days 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 ZETES TSP 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.

Under normal conditions, all external parties have access to the repositories and to the OCSP service, free of charge.

ZETES TSP reserves the right to refuse access, to limit access or to charge a fee for parties who make excessive use of these resources and are thereby obstructing other Relying Parties.

ZETES TSP reserves the right to refuse access, to limit access or to charge a fee for parties who use these resources for the purpose of commercializing value-add services to third parties.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The names used for the certificate for a natural person contains the official given names and surnames as stated on the person's birth certificate, identity card, passport or other acceptable breeder document (fields **givenName** and **surName**) as well as the usual calling name for that person (field **commonName**).

For the purpose of conforming to ETSI EN 319 411-1 and EN 319 411_2 and to the requirements stated in the EU Regulation (EU) No 910/2014, the name attributes in the Qualified Certificates for natural persons are compliant with the ETSI EN 319 412 part 1 and part 2 and Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015.

Many software applications use the **commonName** field to show a choice of certificates to the end user. To help the end user choose the appropriate certificate the **commonName** field may also contain plain wording describing the intended usage of the certificate (i.e. authentication or electronic signature).

Certificate Attribute	Description
serialNumber	**Subject serial number or identifier, t**his is a unique identifier (UUID) as assigned by OVB-OBFG-OAC.
title	**official title of the Subject** as assigned by OVB-OBFG-OAC
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	**Indication of the intended purpose for this certificate + Official name or common name of the Subject + title** The certificate will only contain one instance of commonName. The commonName is intended for a user-friendly representation of the certificate holder's name. The common name is a space separated concatenation of: • the label "**AUT**" or "**QES**" identifying the purpose of the certificate • short-form surname of the Subject • short-form given name of the Subject • the title of the Subject in parentheses (e.g., advocaat) Alternatively, short-form surname of the Subject and/or short-form given name of the Subject may be replaced by the usual calling name
organizationName	**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.

	For the context of this Certificate Policy, the **organizationName** is one of the following: • **“Orde van Vlaamse Balies (KBO 267.393.267)”** • **“Ordre des Barreaux Francophones et Germanophone de Belgique (BCE 850.260.032)”** • **“Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie (BCE-KBO 0240.714.012)”**
organizational Unit	**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 e.g. the name of a Bar Association, an official body within OVB or OBFG, etc.

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of Subscribers

The ZETES TSP Qualified 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 of natural persons. See chapter 3.1.1.

3.1.5 Uniqueness of names

Subject DNs are guaranteed to be unique across the ZETES TSP PKI Domain.

The subject.serialNumber field of the Subject DN is set to the string representation of the UUID which is assigned by the Subordinate RA to each Subject. The Subordinate RA guarantees that any UUID can only be linked to a single uniquely identifiable Subject.

The structure of the UUID is compliant with RFC 4122. The UUID is a 128-bits number and is encoded in the subject.Serialnumber field in the certificate as a 32-character hexadecimal representation of the UUID.

3.1.6 Recognition, authentication, and role of trademarks

No stipulations.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The keys for Secure Cryptographic Devices are generated inside the embedded chip of the Secure Cryptographic Device.

The combination of certified Secure Cryptographic Device and the control of the key generation process guarantees that possession of the private key is guaranteed and that the origin of the private key is known.

The key generation process for the Secure Cryptographic Device will adhere to the conditions and procedures defined in certification criteria for this Secure Cryptographic Device.

For Qualified Certificates, the Secure Cryptographic Device must comply 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.

The key generation process shall comply with the ETSI EN 319 411 parts 1, 2 as applicable for the type of device, purpose and certificate and is further described in the CPS **[ref. 5]**.

3.2.2 Authentication of organization identity

Organization acting as a Subscriber

Organizations acting as Subscriber are authenticated by ZETES TSP 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.

In the case of the present CP, OVB-OBFG-OAC is the organization acting as Subscriber and therefore represents the Subjects.

At the occasion of the Subscriber's Agreement establishment, ZETES TSP has verified the OVB-OBFG-OAC relationship with the Subjects, in particular verify these organization's mandate (as Subscriber) to represent the Subjects, based on ETSI EN 319 411-1 requirements:

- OVB - Orde van Vlaamse Balies composed of the Belgian (Dutch speaking) local Bar Associations as defined in Article 488 of the Belgian Judicial Code
- OBFG - l'Ordre des Barreaux Francophones et Germanophone de Belgique composed of the Belgian (French and German speaking) local Bar Associations as defined in Article 488 of the Belgian Judicial Code
- OAC - "Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie", being the Bar Association as defined in Article 481 of the Belgian Judicial Code

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

The identity of a Subject is authenticated by the RA. In particular, for the present CP, the Subject is already a registered lawyer or a registered associated person with the OVB, OBFG or OAC.

The first step of the registration process in one of three ways:

- Online by the Subject
- in person by the Subject at the Local RA office with which the Subject is associated
- (in specific instances) at the initiative of the Subscriber

The RA ensures authentication and identity validation as described in the TSPS [ref. 4], section 3.3.2.

Authentication of Professional Attributes or Membership Attributes

OVB, OBFG or OAC attests to a Subject's professional attributes such as an official degree, a diploma, a mandate, etc.

OVB, OBFG or OAC attests to a Subject's membership attributes of said organization such as membership, title, association with one or more Bar Associations, etc.

The validation of these attributes is the responsibility of OVB-OBFG-OAC as the Subscriber and OVB, OBFG or OAC as the Subordinate RA. The burden of proof falls upon the Subject and the Subscriber.

3.2.4 Non-verified Subscriber information

A Subject certificate can optionally include the e-mail address of the Subject. It is the responsibility of the Subject or the Subscriber, as the case may be, to provide the correct information. Neither CA nor RA verifies the existence or correctness of the e-mail address.

3.2.5 Validation of authority

OVB-OBFG-OAC as the 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 chapter 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 requests for a new key and certificate for an existing Secure Cryptographic Device and for a Subject who has already been registered. The Secure Cryptographic Device and the existing certificates provide a verifiable association between the re-key request and the previously recorded identity data and attributes of the Subject.

The principles for the identification and authentication of the certificate holder are the same as for the initial registration of the certificate holder. The Subject's identity and membership attributes are verified using the same sources as described in section 3.2.2 and 3.2.3 for initial identification and authentication.

In addition, the authenticity of the Subject's Secure Cryptographic Device is verified and the association of the Security Cryptographic Device with the Subject is verified.

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 for Subject certificates

The following participants may request revocation of a Subject certificate:

- ZETES TSP as operator of the CA and RA
- OVB, OBFG or OAC as the Subordinate RA and as the representative of the Bar Associations (also the Local RAs)
- OVB-OBFG-OAC as the Subscriber
- the Subject

The procedures and conditions for requesting and executing a certificate revocation are described later on in the present CP. These procedures and conditions may be more explicitly defined in internal documents such as the Subscriber Agreement, the Subject Agreement and/or in the Registration Authority Agreement for the Subordinate RA.

Requests that originate from the Subordinate RA or the Subscriber are authenticated by means of a certificate that was issued by the Zetes TSP CA for (S)RA. Authentication can take the form of a signed request or a request which is sent through an authenticated channel.

Requests that originate from the Subject are validated by the L-RA officer if the revocation request is lodged through an L-RA office, or by means of validation of control questions or revocation code if the revocation request is lodged via a call centre.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

The ZETES TSP Qualified CA does not issue certificates to Subjects on an individual basis. The ZETES TSP Qualified CA only issues certificates to Subjects who are entitled to a certificate through explicit approval by and intervention of the Subscriber with which ZETES TSP has entered into a Subscriber Agreement.

The Subscriber and the Subject must comply with the provisions and obligations set forth in the registration form, in the applicable Subscriber Agreement, this Certificate Policy and the Certificate Terms and Conditions.

The CA will only create certificates in response to an authenticated demand from the Central RA infrastructure operated by ZETES TSP. The Central RA will only process certificate requests originating from the authorized and authenticated Subordinate RA or Local RA of the Subordinate RA.

Also see chapter 3.2.3 for more information on who can submit a certificate application.

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 ZETES TSP. For a description of these entities and their respective roles and relationship, please see chapter 1.3.2.

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

ZETES TSP provides the infrastructure and the operational resources for the Central RA. The Central RA relies on the enrolment process performed by OVB, OBFG and OAC as the Subordinate RAs. The Subordinate RAs delegate the enrolment process to their local Bar Associations or 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)

This enrolment process is done in accordance with the rules and methods described in this Certificate Policy and in the internal guidelines and rules for RA entities and the applicable law.

Each RA entity must archive the received or added information for each enrolment. The archive must be kept in a secure location or on a secure system according to the requirements defined in the CPS **[ref. 5]**.

4.1.2.2 Enrolment of Subjects

The Subject Agreement

The Subject is supplied with the following information:

- the registration form including the privacy statement
- reference where to download the CPS and the CP and access to a printed copy
- (the case being) bylaws, notices or other documents provided by the Subscriber (to be defined in the Subscriber Agreement)

- a receipt with information about the certificate(s) and with the Certificate Terms and Conditions, to be signed by the subject before accepting the certificate(s)

The registration form may contain pre-filled information resulting from the online enrolment by the Subject or pre-filled information originating from the Subscriber.

The acceptance by the Subject of the Subject Agreement through signature online with the eID or at the Bar, is a step whereby the Subject accepts

- its 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 ZETES TSP as CSP maintain a retention period of minimum 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 provision of a Secure Cryptographic Device, the suspension/reactivation/revocation of the certificate
- that in case ZETES TSP (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 ZETES TSP and the other PKI Participants, as defined in the Subject Agreement and by national law,
- the Subject has the obligation to inform ZETES TSP of any changes or events that may affect the validity or the content of the certificate

Enrolment Process for Subjects

See also chapter 3.2.3 for more information.

The Local RA (L-RA) collects the required documents and attestations for the subsequent validation of the applicant’s identity and attributes. The L-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 also informs the applicant about his/her rights and obligations.

The Subordinate RA (SUB-RA) is responsible for providing and/or checking information regarding the applicant’s attributes (professional attributes, organisational attributes, etc.). The Subordinate RA checks and completes the enrolment data if necessary. The SUB-RA is responsible for the accuracy of the data that will be incorporated in the certificate request to the Central RA. The SUB -RA is responsible for the correct registration/enrolment of Subjects and for supplying the Central RA with the correct content for the variable fields in the certificate. 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.

Where the process is automated through online application and registration with eID, verification is done based on the presented eID and the automated connection between the C-RA and the SUB-RA regarding the applicant’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.

The C-RA also integrates with the personalisation process for the Secure Cryptographic Device, for the key generation process on the Secure Cryptographic Device and for the certificate request process with the CA. See section for 3.2.1 more details.

An enrolment may cover more than one certificate request. For example, the Subject enrols for a Secure Cryptographic Device which contains one certificate for authentication and one certificate for electronic signature. In such a case, the enrolment procedure pertains to both certificates and both certificates requests will be processed collectively.

Delivery of the Secure Cryptographic Device (smartcard) to the Subjects

ZETES TSP ensures a segregation of the delivery processes for a Secure Cryptographic Device and its associated Activation Data.

The Secure Cryptographic Device is delivered to the Subject in person or by registered mail. The Subject must acknowledge receipt of the device.

The Activation Data (e.g. the PUK and/or PIN) is delivered to the Subject in a tamper evident letter and via a different distribution channel, separate from the Secure Cryptographic Device and at a different point in time.

4.1.2.3 Enrolment of Subscribers

Not applicable. ZETES TSP enters into a Subscriber Agreement with Subscribers but does not enrol Subscribers. Representatives of Subscribers can be enrolled as Subjects should they qualify.

However, the Subscriber plays a role in the enrolment process of Subjects (or in the Subject certificate revocation process). Therefore, the Subscriber Agreement also defines the responsibilities of the Subscriber in relation to the enrolment of the Subject or to the revocation of the Subject certificate and states that:

- the Subscriber acts as the Subordinate RA and Local RAs for the Subscriber's Subjects and in this role the Subscriber is bound by a Registration Authority Agreement.
- the Subscriber accepts responsibility that registration information provided by the Subscriber is complete, valid and up to date,
- that the Subordinate RA and ZETES TSP as CSP maintain a retention period, of **minimum 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 provision of a Secure Cryptographic Device, suspension/reactivation/revocation of the certificate
- that in case ZETES TSP (as CA and RA) or the Subscriber 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 ZETES TSP and the other PKI Participants, as defined in the Subject Agreement and by national law,
- the Subscriber has the obligation to inform ZETES TSP of any changes or events that may affect the validity or the content of the certificate of a Subject

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Local Registration Authority performs identification and authentication of the Subjects according to the procedure defined. The Local Registration Officers are assigned by the Local RA and the Subordinate RA.

The Local RA collects and validates the Subject's identity information and attributes information and forwards this to the Subordinate RA for additional validation and further processing.

See also 4.1.2.

4.2.2 Approval or rejection of certificate applications

Approval or rejection of certificate applications is undertaken by the Subordinate RA. Also, ZETES TSP as 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 ZETES TSP as CSP.

Certificate requests are 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 ZETES TSP as CSP.

4.2.3 Time to process certificate applications

The RA will make a best effort to process each certificate application within a reasonable time. The Subject will be informed as soon as possible about the status of the application and, if the application was accepted, when the certificate will be available.

Because the certificates are stored on a Secure Cryptographic Device, applications may be processed differently for a certificate on a new Secure Cryptographic Device and applying for certificates to be stored on an existing Secure Cryptographic Device.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The certificate is issued as part of the initial personalisation process or a post-issuance personalisation process of the Secure Cryptographic Device. The CA will only receive certificate requests from the Central RA in conjunction with the personalisation system and management system for the Secure Cryptographic Devices.

For every certificate request, the CA shall perform the checks and actions defined in the CPS **[ref. 5]**.

4.3.2 Notification of issuance of certificate

If the certificate is issued as part of the initial personalisation process of the Secure Cryptographic Device, the Subject receives the notification as part of the delivery procedure of the Secure Cryptographic Device.

If the certificate is issued for an already existing Secure Cryptographic Device, i.e. as part of a post-issuance update of the Secure Cryptographic Device, then the Subject participates in the post-issuance update procedure of the Secure Cryptographic Device and is notified de-facto of the issuance of the certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate is accepted by the Subscriber and the Subject either

- upon completion of the handover procedure or delivery procedure for a new Secure Cryptographic Device to the Subject.
- upon completion of the post-issuance update procedure for an existing Secure Cryptographic Device

The Subject and the Local RA officer sign a Subject Agreement document which combines:

- the request form to obtain (a) new certificate(s) including reference the privacy policy
- a declaration of acceptance by the Subject of the new certificate(s)
- declaration of and acceptance by the Subject of the Certificate Terms and Conditions

Where the process is automated through online application and registration with eID, the Subject will sign with the electronic signature the Subject Agreement.

The Subscriber, Subordinate RA, Local RA and the Subject all have the right to reject the certificate or the Secure Cryptographic Device and return the Secure Cryptographic Device, provided at least one of the following objections applies:

- the information in the certificate is incorrect,
- the information in the certificate became invalid since the date of registration,
- the Secure Cryptographic Device shows signs of damage or tampering,
- the Secure Cryptographic Device malfunctions or cannot be activated,
- the letter with secret information for the Secure Cryptographic Device shows signs of tampering,
- the delivery procedure for either the Secure Cryptographic Device or the letter with secret information was not respected,
- the Subject cannot take receipt of the Secure Cryptographic Device,
- loss of entitlement of the Subject.

Rejection of the Secure Cryptographic Device implies rejection of all the Subject's certificates that are stored on the device.

Rejection of one or more Subject's certificates that are stored on the Secure Cryptographic Device, implies revocation of these certificates.

Obligations of the Subject and the SRA in case of rejection:

- the Secure Cryptographic Device must be destroyed or must be returned to the CA for destruction
- the SRA must execute the revocation of the certificates

4.4.2 Publication of the certificate by the CA

See section 2 for information on the publication of the certificate.

4.4.3 Notification of certificate issuance by the CA to other entities

The CA will notify the Subscriber of the issuance of the certificate, by means of notification method stipulated in the Subscriber Agreement.

Regarding notification of the Subject, see chapter 4.3.2.

4.5 Key pair and certificate usage

4.5.1 Subject private key and certificate usage

The Subject must use the private keys and use the certificates for the purposes described in chapter 1.4 .

ZETES TSP Qualified CA issues certificates for keys stored on Secure Cryptographic Devices that guarantee that:

- the private key cannot be extracted from the Secure Cryptographic Device
- the private key is under the (sole) control of the Subject
    - by means of a secret code (PIN, password or passphrase)
    - or by an equivalent mechanism such as biometric Match on Card

The Subject is bound by the conditions and obligations mentioned the Subject Agreement, which includes this CP, and the CPS. The Subject must protect the Secure Cryptographic Device and any associated Activation Data (e.g. password, PIN code, PUK code, etc.) or other information against loss, theft, disclosure, compromise or modification.

Once the Secure Cryptographic Device or associated Activation Data is delivered to the Subject, the Subject is personally responsible for:

- using the keys only for the intended use as encoded in the certificates

- using tools that can correctly interpret the key usage as encoded in the certificate and that respect the key usage conditions
- correct usage of the Secure Cryptographic Device
- not sharing the Secure Cryptographic Device with another person
- setting Activation Data that is unique
- keeping these secret information confidential
- safe storage of any document or medium containing transcripts of part or all of the associated Activation Data
- separation of storage for the Secure Cryptographic Device and the associated Activation Data
- not disclosing the Activation Data to another person

The Subject will be provided with guidelines and instructions for the specific Secure Cryptographic Device.

4.5.2 Relying Party public key and certificate usage

Relying Parties should not rely on a (Qualified) 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 in the applicable Certification Practice Statement and Certificate Policy.
- Successfully perform public key operations as a condition of relying on a (Qualified) 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 by ZETES TSP:
  - the Certificate Revocation Lists (CRLs) (see also section 4.9.6)
  - the OCSP service
- if the certificate has been revoked, has been suspended or has expired:
  - immediately stop trusting the certificate
  - 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 regard to the use of the (Qualified) 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

Under the present policy the Subject certificates are not renewed, i.e. the CA does not issue certificates for replacing existing certificates for existing keys on already issued Secure Cryptographic Devices. Situations that may require certificate renewal are handled as a request for replacement of the Secure Cryptographic Device or as requests for certificate re-keying.

4.7 Certificate re-key

The certificate re-key procedure is the commissioning of a new key and new certificate for the following use cases:

- replace a blocked key and its certificate
- replace a revoked certificate and its key
- replace an existing key/certificate that is about to expire or has expired
- replace an existing key/certificate when the card holder's identity data or attributes have changed

Certificate re-keying for Subject certificates involves

- revocation of the preceding certificate if it is not expired or revoked already,
- post-issuance personalisation of the Secure Cryptographic Device:
  - commissioning of an unused pre-generated key pair or the generation of a new key pair,
  - creation of a new certificate,
  - installation of the new certificate on the Secure Cryptographic Device.

The certificate re-key process uses the previously registered identity data and attributes of the certificate holder.

The re-keying process includes controls such as proof of identity and security mechanisms such as smartcard secure messaging protocols to ensure that

- the identity of the certificate holder is verified before issuing the new certificate
- the identity data and attributes of the certificate holder are up to date
- the new key is generated on an authentic Secure Cryptographic Device
- the new certificate is issued for the certificate holder who is associated with the Secure Cryptographic Device

4.8 Certificate modification

Under the present policy the Subject certificates are not modified,, i.e. the CA does not issue modified certificates to replace existing certificates for existing keys on already issued Secure Cryptographic Devices. Situations that may require certificate modification are handled as a request for replacement of the Secure Cryptographic Device or as requests for certificate re-keying.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Revocation is needed for the following reasons:

- The Subject has not collected the Secure Cryptographic Device in due time, as specified in the present Certificate Policy or Certificate Terms and Conditions
- The PMA, CA, RA, Subscriber or the Subject itself
  - have reason to believe or suspect that the Subject's private key has been compromised;
  - have reason to believe or suspect that the secret information pertaining to the Secure Cryptographic Device and the private key(s) has been compromised or is malfunctioning;
  - have reason to believe that the certificate has been issued or used not in a manner that is in accordance with the applicable rules (e.g. rules expressed in the present document or in the CP have been violated);
- The Secure Cryptographic Device is
  - lost;
  - out of order or does not function properly;
- The information in the certificate is no longer correct;
- The Subscriber may decide to request revocation of its Subject's certificate(s) for reasons internal to the Subscriber, in compliance with the Subscriber Agreement and the Subject Agreement (e.g. a Subject's entitlement certified has been withdrawn because the Subject is no longer an employee/member/participant of the Subscriber);

- The Subject may decide to request revocation of its certificate(s) for reasons internal to the Subject, in compliance with the Subject Agreement;

ZETES TSP as a certification service provider (CSP), under prior or explicit approval of the PMA, must revoke a certificate in exceptional circumstances as defined in the governing law, e.g. in case ZETES TSP is informed on strong suspicion that:

- the registration information was wrong or falsified,
- there is evidence that the information in the certificate is no longer correct,
- the confidentiality of the private key was compromised,
- the entity to which the certificate is issued (the Subject) no longer exists or will cease to exist, e.g. the person is deceased, was struck from the population register, etc.
- in case of a court order,
- in case ZETES TSP terminates its certificate service provider activities without handing over to another CSP with similar quality and security levels.

4.9.2 Parties that can request revocation

A certificate revocation request for Subject certificate can be submitted by the PMA, CA, RA, the Subscriber or the Subject to which the certificate was issued or any entity entitled to represent the Subject according to the present Certificate Policy.

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

4.9.3 Procedure for revocation request

Procedure for revocation of Subject certificates - request by the Subject

A Subject can request revocation of its certificate(s) via the Subscriber or via an automated procedure under control of the SRA. The following possibilities are offered under the present CP:

CHANNEL	SUBJECT AUTHENTICATION MECHANISMS
SUBSCRIBER	**identification** • a combination of name, date of birth, member number, card number, etc. **authentication mechanisms** • an official identification document such as a national ID card or a passport • a pre-defined revocation authentication code
CALL CENTER	**identification** • a combination of name, date of birth, member number, card number, etc. **authentication mechanisms** • control questions (personal information other than the identifiers) • a pre-defined revocation authentication code

A revocation request will be executed only if the following conditions are met:

- the request is submitted via an appropriate channel

- the requester can be identified and authenticated as defined in the Subscriber Agreement
- the reason for revocation is acceptable as defined in the Subscriber Agreement or in the applicable law

Procedure for revocation of Subject certificates - request by the Subscriber

The Subscriber, in its role as the Subordinate RA, can request revocation of a Subject's certificate(s). The procedures and access points for requesting revocation are described in the Subscriber Agreement and in the Registration Authority Agreement. The following possibilities are offered under the present CP:

CHANNEL	SUBSCRIBER AUTHENTICATION MECHANISMS
SUB-RA internal membership register management system	**identification** • a combination of name, organization and role **authentication mechanisms** • logon to the internal system using a valid and appropriate certificate

A revocation request will be executed only if the following conditions are met:

- the request is submitted via an appropriate channel
- the requester can be identified and authenticated as defined in the Subscriber Agreement
- the requester is authorized to request revocation of the certificate as defined in the Subscriber Agreement
- the reason for revocation is acceptable as defined in the Subscriber Agreement or in the applicable law

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 1 day following receipt of the revocation request.

4.9.6 Revocation checking obligations for Relying Parties

Relying parties must use at least one of the services for checking certificate status information that are made available by ZETES TSP. 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 or not to trust the certificate, regardless of the availability of the certificate status information services.

See section 2.2 and section 4.5.2.

4.9.7 CRL issuance frequency

The ZETES TSP Qualified CA shall issue CRLs and delta-CRLs at pre-defined intervals or ad hoc when needed. The CRL/delta-CRL is refreshed at least every 24 hours.

The CRL and delta-CRL shall be signed and time-marked by the CA.

4.9.8 Maximum latency for CRLs

The issuance frequency and latency for CRLs is such that revoked certificates are included in a CRL or delta-CRL within 60 minutes of the actual revocation.

4.9.9 On-line revocation/status checking availability

ZETES TSP maintains an Online Certificate Status Protocol (OCSP) service:

http://ocsp.tsp.zetes.com

See section 4.10 for more information.

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

ZETES TSP 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

For revocation of Subject certificate, the Subject is notified of the revocation of a certificate via e-mail. The contact information for the Subject is kept up to date by the Subordinate RA. A registered Subject has the obligation to inform the Subordinate RA of any change in contact information.

Revocation of Subject certificates is not advertised to Relying Parties.

Revocation of CA certificates or certificates for PKI components which are of immediate relevance for Relying Parties will be advertised during an appropriate period on the appropriate ZETES TSP repository pages:

https://repository.tsp.zetes.com or https://repository.confidens.zetes.com

http://crt.tsp.zetes.com or http://crt.confidens.zetes.com

http://crl.tsp.zetes.com or http://crl.confidens.zetes.com

4.9.12 Special requirements regarding key compromise

No stipulations.

4.9.13 Circumstances for suspension

Suspension is currently not supported.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 imits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

The ZETES TSP Qualified CA shall provide two services for checking the status of the Subject certificates issued by the ZETES TSP Qualified CA as well as the status of the ZETES TSP Qualified CA's own CA certificates:

- Certificate Revocation Lists
- Online Certificate Status Protocol service

CRLs and delta-CRLs Download Service

CRLs and delta -CRLs are published at regular intervals on the CRL distribution point at http://crl.tsp.zetes.com.

CRLs and delta-CRLs shall be published at regular intervals on the general CRL distribution point at http://crl.tsp.zetes.com and/or a CRL distribution indicated in the certificate (see the Certificate Policy and certificate profile for the certificate). CRLs or delta-CRLs may be renewed 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 http://ocsp.tsp.zetes.com and is synchronised with the latest certificate status information.

The OCSP services provide certificate status information for Subject certificates on behalf of the Zetes TSP Qualified CA 001. The OCSP services provide certificate status information for the Zetes TSP Qualified CA 001 root-signed certificate on behalf of the Zetes TSP Root CA 001.

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 certificate profiles, see section **Error! Reference source not found.**.

Retention period for Certificate Status Information after expiration of the certificates

Certificate status information in CRLs and the OCSP service shall be updated at least until all certificates that were issued by the respective CA have expired. For qualified certificates, the certificate status information shall remain available beyond the validity period of the certificate, until the issuing CA certificate has expired.

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://tsp.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 ZETES TSP or any other reason, Zetes SA 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.

ZETES TSP 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

No key escrow and no key recovery. The usage of the certificates issued by the ZETES TSP Qualified CA is authentication and/or electronic signature, therefore key escrow is not recommended. Key escrow is not compliant with the applicable regulations and legislation for electronic signatures.

Due to the obligatory use of a Secure Cryptographic Device it is technically impossible and forbidden to extract the key pair from the device, therefore key escrow is not compliant with the applicable regulations and legislation for electronic signatures.

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

Non-technical security controls (that is, physical, procedural, and personnel controls) used by ZETES CSP to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving are described in section 5 of the Certification Practices Statement [Ref. 5].

Provisions on compromise and disaster recovery, and on termination of all or parts of the ZETES TSP activities are also described in section 5 of the above mentioned CPS [Ref. 5].

6 TECHNICAL SECURITY CONTROLS

For description of the technical security controls (including secure key management) applicable to the ZETES CPS components (CA, RA and other PKI components services), refer to section 6 of the CPS **[ref. 5]**.

6.1 Key pair generation and installation

6.1.1 Subject Key pair generation

The key pairs for Subjects are generated by Zetes on behalf of ZETES TSP on-board a Secure Cryptographic Device as an integrated part of the Secure Cryptographic Device personalisation service. They are *de facto* delivered to the Subject at the occasion of the Secure Cryptographic Device hand-over. Post-issuance key generation is allowed if the Secure Cryptographic Device provides the security mechanisms to guarantee the security of the key generation process performed in the environment of the Local RA.

6.1.2 Private key delivery to Subscriber or Subject

The key generation process for a Subject is described in section 6.1.1.

There are no private keys issued for the Subscriber and no certificates are issued to the Subscriber.

6.1.3 Public key delivery to certificate issuer

ZETES TSP Qualified CA generates the key on the Secure Cryptographic Devices it personalises, the subject's public key is de facto in its possession. Technical controls are provided in the CPS.

6.1.4 CA public key delivery to Relying Parties

ZETES TSP CA certificates are stored on the Secure Cryptographic Device, which can be considered as a secure means of delivery to the Subject.

For the benefit of the Relying Parties, the ZETES TSP CA certificates shall be published on a secure web site:

https://repository.tsp.zetes.com or 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 CA that is external to the ZETES TSP CA hierarchy.

The authentic "thumbprint" of the ZETES TSP CA certificates shall be published in a document in PDF/A format.

Relying parties may contact ZETES TSP via e-mail at info@tsp.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

Algorithms and key sizes:

End entity Secure Cryptographic Device	RSA2048/RSA3072/ECC384	generated and used on the SCD
CA HSM	RSA4096	generated and used on HSM
OCSP HSM	RSA2048/ECC256	generated and used on HSM

All certificates shall be signed using SHA256withRSA.

ZETES TSP reserves the right to introduce other algorithms and protocols than SHA256withRSA or longer key lengths in the future. This may include Elliptic Curve algorithms instead of RSA and other hash algorithms.

ZETES TSP is not in any way held to continue using the current algorithms, protocols or key lengths for any purpose, should ZETES TSP 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

Keys for Secure Cryptographic Devices are generated on the device itself and meet the cryptographic quality requirements laid down for Qualified Signature Creation Devices.

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

ZETES TSP shall ensure that the key usage properties encoded in the certificates correspond with the intended use of the certificates as described in the Certification Practice Statement and in the present Certificate Policies.

For details about the encoded key usage, see section 7.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

For the purpose of a Qualified Electronic Signature (QES) with a certificate that adheres to the policy [QCP-n-qscd], the Secure Cryptographic Device complies with the requirements for a Qualified Signature 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).

For more information, see the Certificate Practice Statement **[ref. 5]**.

6.2.2 Private key multi-person control

Not applicable. The Secure Cryptographic Device is only to be used by the designated Subject.

6.2.3 Private key escrow

Private keys cannot and are never extracted from the Secure Cryptographic Device on which they are generated. Private keys are never put in escrow.

6.2.4 Private key backup

Private keys on a Secure Cryptographic Device are generated on-board the device and cannot be backed up.

6.2.5 Private key archival

Private keys on a Secure Cryptographic Device are generated on-board the device and cannot be extracted for backup, escrow or archival.

6.2.6 Private key transfer into or from a cryptographic module

Private keys on a Secure Cryptographic Device cannot be transferred.

6.2.7 Private key storage on cryptographic module

Private keys on a Secure Cryptographic Device are stored in secure memory.

See CPS **[ref. 5]** for more details.

6.2.8 Method for activating private keys

Activation data for Secure Cryptographic Device consist of PIN codes, PUK codes or are derived from the biometric characteristics of the Subject (e.g. fingerprint for biometric Match on Card). PIN codes and PUK codes are provided to the Subject in a protective tamper-evident container such as a PIN letter and/or sealed envelope.

6.2.9 Method of deactivating private key

A private key for a Qualified Electronic Signature can only be used once when it is activated and it is automatically deactivated after it is used or if was not used as the next action after the activation process.

6.2.10 Method of destroying private key

The private key can be blocked or even decommissioned (irreversibly blocked) by repeatedly providing an incorrect PIN or PUK code. Some Secure Cryptographic Device may have a special function to (irreversibly) block, decommission or erase a key.

6.2.11 Capabilities and Rating of the Cryptographic Module

Not applicable. No HSM are delivered to end-users.

6.3 Other aspects of key pair management

6.3.1 Public key archival

ZETES TSP shall maintain an internal archive of all CA public keys and all public keys certified by the ZETES TSP Qualified CA in the form of the certificates that contain the public key.

6.3.2 Certificate operational periods and key pair usage periods

The ZETES TSP Qualified CA shall not issue certificates that exceed the certificate expiration date of the CA certificate.

The key usage period of a CA key shall be aligned with the expiration date / lifetime of the certificates issued with that key.

6.4 Activation data

See section 6.2.8.

6.5 Computer security controls

ZETES TSP ensures computer security controls described in the CPS **[ref. 5]**.

6.6 Life cycle technical controls

ZETES TSP ensures life cycle technical controls described in the CPS **[ref. 5]**.

6.7 Network security controls

ZETES TSP ensures network security controls described in the CPS **[ref. 5]**.

6.8 Time-stamping

See the TSPS [ref. 4].

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profiles

The certificates issued by the Zetes TSP Qualified CA are interoperable and adhere to the industry standards ISO/IEC 9594-8 also known as the ITU X.509 standard.

7.1.1 The Zetes TSP CA hierarchy

The certificates described in this Certificate Policy are issued by the Zetes TSP Qualified CA 001.

The CA hierarchy for these certificates is the following:

```
ZETES TSP Root CA 001
          |   Subject serialNumber = 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 for the Zetes TSP Certification Authorities.

7.1.2 Certificate Profile for NCP+ on smartcards

This certificate profile is for a Normalised Certificate issued to a natural person (the Subject) and associated with a key pair on a Secure Cryptographic Device. The key usage is restricted to TLS client authentication purposes and/or digital signature for e-mails.

The certificate profile is compliant with the certificate profile type “NCP+” as defined in ETSI EN 319 412-1 and ETSI EN 319 412-2.

The key generation process is performed and controlled by Zetes TSP according to the registration and issuing process and procedures described in the Certification Practice Statement and this Certificate Policy.

The key pair is generated on-board the embedded chip of the Secure Cryptographic Device. Only the public part of the key pair can be extracted from the chip of the Secure Cryptographic Device, for the purpose of creating the associated certificate. The private part of the key pair cannot be exported or extracted.

Table 1 ZETES TSP NCP+ certificate for natural persons - for the Subscriber OVB-OBFG-OAC

certificate profile **ZETES TSP NCP+ certificate for natural persons for the Subscriber OVB-OBFG-OAC – on smartcards** **certificate policy OID: 1.3.6.1.4.1.47718.2.1.2.2.1.10** **certificate profile OID: 1.3.6.1.4.1.47718.2.1.3.2.1.10** version 1.1				
ATTRIBUTES				
Version		-	MS	**0x02** *(= X.509 certificate version 3)*
Serial Number		-	MD	< 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 >
Signature Algorithm	**algorithm**	-	MS	**sha256WithRSAEncryption**
Signature Value		-	MD	< the signature created by the CA >
SubjectPublicKeyInfo	**algorithm**	-	MS	**RSA2048** or **RSA3072** or **ECC384**
	subjectPublicKey	-	MD	value of the public key
Validity	**notBefore**	-	MD	< certificate validity start date >
	notAfter	-	MD	< certificate validity start date + certificate validity period >
Issuer	**serialNumber**	-	MS	**001**
	commonName	-	MS	**ZETES TSP QUALIFIED CA 001**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
Subject	**serialNumber**	-	MD	**Subject serial number or identifier** This is a unique identifier (UUID) as assigned by OVB-OBFG-OAC.
	title	-	MD	**title of the Subject** *as assigned by the SUB-RA/LRA* Dutch: “**advocaat**” “**staff member**” French : „**avocat**“ „**staff member**“ German : „**Rechtsanwalt**“ „**staff member**“
	givenName	-	MD	**official given name(s) of the Subject** space (“ “) separated full-form concatenation of given names, identical to how it is obtained from the breeder document that was used to register the Subject
	surname	-	MD	**official surname(s) of the Subject** space (“ “) separated full-form concatenation of surnames, identical to how it is obtained from the breeder document that was used to register the Subject
	commonName	-	MD	**Indication of the intended purpose for this certificate + Official name or common name of the Subject + title** The format is a space separated concatenation of: ● the label “**AUT**” or “**CERT**” identifying the purpose of the certificate ● short-form surname of the Subject ● short-form given name of the Subject ● the title of the Subject in parentheses (e.g., advocaat) Alternatively, short-form surname of the Subject and/or short-form given name of the Subject may be replaced by the usual calling name
	countryName	-	MD	**nationality of the Subject** 2-character ISO 3166 country code
	emailAddress	-	OD	**e-mail address of the Subject**
	organizationName	-	MD	**The official or registered name of the Subscriber,** either “**Orde van Vlaamse Balies (KBO 267.393.267)**” or “**Ordre des Barreaux Francophones et Germanophone de Belgique (BCE 850.260.032)**” or **“Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie (BCE-KBO 0240.714.012)”**
	organizationalUnitName	-	OD	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 e.g. the name of a Bar Association, an official body within OVB or OBFG, etc.
EXTENSIONS -- Authority Properties				
authorityKeyIdentifier	**keyIdentifier**	-	MS	< SHA-1 hash of the public key of the CA (as specified in RFC 5280) >
authorityInfoAccess	**accessMethod**	-	MS	**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	-	MS	**http://crt.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crt** or **http://crt.confidens.zetes.com/ZETESTSPQUALIFIEDCA001.crt** *(001 is the 3-digit serialNumber of the ZETES TSP QUALIFIEDCA 001)*
	accessMethod	-	MS	**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	-	MS	**http://ocsp.tsp.zetes.com** or **http://ocsp.confidens.zetes.com**
CRLDistributionPoint	**distributionPointName**	-	MS	-
	fullname	-	MS	**http://crl.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crl** or **http://crl.confidens.zetes.com/ZETESTSPQUALIFIEDCA001.crl** *(001 is the 3-digit serialNumber of the ZETES TSP QUALIFIEDCA 001)*
FreshestCRL	**distributionPointName**	-	MS	
	fullname	-	MS	**http://crl.tsp.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl** or **http://crl.confidens.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl** *(001 is the 3-digit serialNumber of the ZETES TSP QUALIFIED CA 001)*
EXTENSIONS -- Subject Properties				
subjectKeyIdentifier	**keyIdentifier**	-	MD	< 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	**digitalSignature**	c	MS	true
Extended Key Usage	**Client Authentication**	nc	MS	**OID: 1.3.6.1.5.5.7.3.2** {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) clientAuth(2)}
	eMailProtection	nc	OS	**OID: 1.3.6.1.5.5.7.3.4** {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) eMailProtection(4)}
certificatePolicies	**policyIdentifier**	-	MS	**OID: 1.3.6.1.4.1.47718.2.1.2.2.1.10** {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) zetes(47718) zetes-tsp(2) cs(1) cert-policy(2) qca(2) ncp+(1) ovb-obfg-oac(10) }
	policyQualifierID	-	MS	Id-qt-1 (**CPS**)
	qualifier	-	MS	**https://repository.tsp.zetes.com** or **https://repository.confidens.zetes.com**
	policyQualifierID	-	MS	Id-qt-2 (**User Notice**)
	displayText	-	OS	"**Enhanced normalized certificate for authentication as a natural person using a Secure Device.**"
	policyIdentifier	-	MS	**OID: 0.4.0.2042.1.2** {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)}
basicConstraints	**subjectType**	c	MS	**false** (CA = false)

7.1.3 Certificate Profile for QCP-n-qscd on smartcards

This certificate profile is for a Qualified Certificate issued to a natural person (the Subject) for the purpose of creating Qualified Electronic Signatures.

The certificate profile is compliant with the certificate profile type "QCP-n-qscd" as defined in ETSI EN 319 412-1, ETSI EN 319 412-2 and ETSI EN 319 412-5.

The key usage field in the certificate is set to "non-repudiation" and the certificate extensions include the QCStatements as defined in ETSI EN 319 412-5 to indicate that the certificate is to be used exclusively for the creation of Qualified Electronic Signatures.

The certificate is associated with a key pair on a Secure Cryptographic Device that meets the requirements for a Qualified Signature Creation Device (QSCD) device as defined in Regulation (EU) 910/2014 and is certified according to a Protection Profile as defined in ETSI EN 419 211. See chapter 1.1 for more details on QSCD.

The key generation process is performed and controlled by Zetes TSP according to the registration and issuing process and procedures described in the Certification Practice Statement and the Certificate Policy (this document).

The key pair is generated on-board the embedded chip of the QSCD. Only the public part of the key pair can be extracted from the chip of the QSCD, for the purpose of creating the associated certificate. The private part of the key pair cannot be exported or extracted from the QSCD.

The certificate validity period is maximum 36 months.

Table 2 ZETES TSP QCP-n-qscd certificate profile for natural persons - for the Subscriber OVB-OBFG-OAC

certificate profile **ZETES TSP QCP-n-qscd certificate for natural persons - for the Subscriber OVB-OBFG-OAC – on smartcards** **certificate policy OID: 1.3.6.1.4.1.47718.2.1.2.2.3.10** **certificate profile OID: 1.3.6.1.4.1.47718.2.1.3.2.3.10** version 1.1				
ATTRIBUTES				
Version		-	MS	**0x02** *(= X.509 certificate version 3)*
Serial Number		-	MD	< 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**	-	MS	**sha256WithRSAEncryption**
Signature Value		-	MD	< the signature created by the CA >
subjectPublicKeyInfo	**algorithm**	-	MS	**RSA2048** or **RSA3072**
	subjectPublicKey	-	MD	value of the public key
Validity	**notBefore**	-	MD	< certificate validity start date >
	notAfter	-	MD	< certificate validity start date + certificate validity period >
Issuer	**serialNumber**	-	MS	**001**
	commonName	-	MS	**ZETES TSP QUALIFIED CA 001**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
Subject	**serialNumber**	-	MD	**Subject serial number or identifier** This is a unique identifier (UUID) as assigned by OVB-OBFG-OAC.
	title	-	MD	**title of the Subject** as assigned by the SUB-RA/LRA Dutch : “**advocaat**” French : “**avocat**“ German : “**Rechtsanwalt**“
	givenName	-	MD	**official given name(s) of the Subject** space (“ “) separated full-form concatenation of given names, identical to how it is obtained from the breeder document that was used to register the Subject
	surName	-	MD	**official surname(s) of the Subject** space (“ “) separated full-form concatenation of surnames, identical to how it is obtained from the breeder document that was used to register the Subject
	commonName	-	MD	**Indication of the intended purpose for this certificate + Official name or common name of the Subject + title** The format is a space separated concatenation of: ● the label “**QES**” identifying the purpose of the certificate ● short-form surname of the Subject ● short-form given name of the Subject ● the title of the Subject in parentheses (e.g., advocaat) Alternatively, short-form surname of the Subject and/or short-form given name of the Subject may be replaced by the usual calling name
	countryName	-	MD	**nationality of the Subject** 2-character ISO 3166 country code
	emailAddress	-	OD	**e-mail address of the Subject**
	organizationName	-	MS	**The official or registered name of the Subscriber,** either “**Orde van Vlaamse Balies (KBO 267.393.267)**” or “**Ordre des Barreaux Francophones et Germanophone de Belgique (BCE 850.260.032)**” or **“Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie (BCE-KBO 0240.714.012)”**

	organizationalUnitName	-	OD	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 e.g. the name of a Bar Association, an official body within OVB or OBFG, etc.
EXTENSIONS -- Authority Properties				
authorityKeyIdentifier	**keyIdentifier**	-	MS	< SHA-1 hash of the public key of the CA (as specified in RFC 5280) >
authorityInfoAccess	**accessMethod**	-	MS	**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	-	MS	**http://crt.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crt**
	accessMethod	-	MS	**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	-	MS	**http://ocsp.tsp.zetes.com**
CRLDistributionPoint	**distributionPointName**	-	MS	-
	fullname	-	MS	**http://crl.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crl**
FreshestCRL	**distributionPointName**	-	MS	
	fullname	-	MS	**http://crl.tsp.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl**
EXTENSIONS -- Subject Properties				
subjectKeyIdentifier	**keyIdentifier**	-	MD	< 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	MS	true
certificatePolicies	**policyIdentifier**	-	MS	**OID: 1.3.6.1.4.1.47718.2.1.2.2.3.10** { iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) zetes(47718) zetes-tsp(2) cs(1) cert-policy(2) qca(2) qcp-n-qscd(3) ovb-obfg-oac(10) }
	policyQualifierID	-	MS	Id-qt-1 (**CPS**)
	qualifier	-	MS	**https://repository.tsp.zetes.com**
	policyQualifierID	-	MS	Id-qt-2 (**User Notice**)
	displayText	-	MS	"**Qualified Certificate for Qualified Electronic Signature by a natural person using a QSCD.**"
	policyIdentifier	-	MS	**OID: 0.4.0.194112.1.2** {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd(2)}
basicConstraints	**subjectType**	c	MS	**false** (CA = false)
QualifiedCertificateStatement		-	MS	**OID: 1.3.6.1.5.5.7.1.3**
	qcCompliance	-	MS	**OID: 0.4.0.1862.1.1** {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1)}
	qcType	-	MS	**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	-	MS	**OID: 0.4.0.1862.1.4** {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) QcSSCD(4)}
QcPDS	**PdsLocations**	-	MS	**OID: 0.4.0.1862.1.5** sequence of URL(s) to the PKI Disclosure Statement (PDS) established in accordance with ETSI EN 319 411-2.
	url	-	MS	**https://pds.tsp.zetes.com** *(URL of the web site with the Public Disclosure Statement in English)*
	language	-	MS	**en** *(ISO 639-1 language code)*
	url	-	OS	**https://pds.tsp.zetes.com** *(URL of the web site with the Public Disclosure Statement in Dutch)*
	language	-	OS	**nl** *(ISO 639-1 language code)*
	url	-	OS	**https://pds.tsp.zetes.com** *(URL of the web site with the Public Disclosure Statement in French)*
	language	-	OS	**fr** *(ISO 639-1 language code)*
	url	-	OS	**https://pds.tsp.zetes.com** *(URL of the web site with the Public Disclosure Statement in German)*
	language	-	OS	**de** *(ISO 639-1 language code)*

7.1.4 Certificates for Test Purposes

Zetes TSP shall provide the capability to allow third parties to check and test the various certificate types.

For this purpose, Zetes TSP shall publish the test certificates and private keys in PKCS#12 format in its public repository. The test certificates shall be made available in a variety of certificate status conditions (valid, expired and revoked).

The test certificates shall clearly indicate that they are for testing purposes (a.o. in the subject name, organization name, Zetes TSP proprietary policy OID and in the user notice statement):

- **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”

  xxxxxx is a 6-digit number, unique for each certificate
- 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 is set to “test.test@example.com”
- **subject Organization and OrganizationalUnit** are the same as the real certificates but prefixed with “TEST “
- special **URL**s in test certificates *:
  - http://crt.test.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crt
  - http://ocsp.test.tsp.zetes.com
  - http://crl.test.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crl
  - http://crl.test.tsp.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl
- identical **URLs** in test certificates:
  - https://repository.tsp.zetes.com
  - https://pds.tsp.zetes.com

  these URL remain identical as those in the real certificates because the certificate must point to the real CP/CPS/PDS 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):**

real OID CP QES certificates:	1.3.6.1.4.1.47718.2.1.2.2.3.10
test OID CP QES certificates:	2.999.1.3.6.1.4.1.47718.2.1.2.2.3.10
real OID CP AUT certificates:	1.3.6.1.4.1.47718.2.1.2.2.1.10
test OID CP AUT certificates:	2.999.1.3.6.1.4.1.47718.2.1.2.2.1.10

- **QC Statements**

  Test certificates contain the same key usage attributes and QC Statement attributes as the real certificates. To distinguish test certificates from real certificates, the **User Notice** attribute will contain a clear statement that the certificate is intended for test purposes only.

** Remark: The URLs in the test certificates that refer to the CRL, CA crt download and the OCSP service are 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 Zetes TSP these URLs may be diverted to another resource, e.g. in case of abusive use of the test certificates.*

7.2 CRL profile

For more information, see the Certification Practice Statement **[ref. 5]**.

7.3 OCSP profile

For more information, see the Certification Practice Statement **[ref. 5]**.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Besides the supervision by the Belgian national supervisory body (FPS Economy, SMEs, Self-employed and Energy - Quality and Safety), ZETES TSP through its PMA shall organize with regards to its CA activities a compliance audit to ensure that it meets requirements, standards, procedures and service levels according to its CPS **[ref. 5]**.

In case of a major security incident, the national Supervisory Body shall be notified of the incident.

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

9 OTHER BUSINESS AND LEGAL MATTERS

The CPS, the present CP and the Subscriber Agreement constitute the main set of terms and conditions for the provision and use of ZETES TSP Qualified CA's offering.

The Subscriber 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 of its SCD and are accepted by the Subject as part of its Subject Agreement.

A Relying Party not having executed any Subject Agreement can rely on all information available in the CPS and the present CP. Such information is also summarized for the Relying Party's convenience in the Public Disclosure Statement (https://pds.tsp.zetes.com). The Relying Party shall be deemed to have tacitly accepted the TSP terms and conditions incorporated in the relevant public documents such as CPS and CP upon relying on the Certificate.

The sections below provide useful information about certain terms and conditions governing the provision or use of ZETES TSP Qualified CA's offering.

9.1 Fees

ZETES TSP Qualified CA services such as but not limited to:

- certificate issuance and certificate renewal,
- certificate validation,
- certificate suspension, certificate revocation, etc.

will be offered as paid services to the Subscriber and its Subjects.

ZETES TSP refund policy is very clear: no refund is possible. Signing of the above-mentioned commercial agreements with the Subscriber as well as the Subscriber Agreement, including implicit acceptance of ZETES TSP CPS, specific CP and CTC, will launch the Trusted Services for that specific Subscriber including certificate issuance and services towards identified Subjects. No refund will be allowed or accepted.

9.2 Financial responsibility

9.2.1 Insurance coverage

Each PKI Participant not being a Subscriber or a Relying Party of the ZETES TSP Qualified CA shall contract an insurance policy covering the risks identified in the insurance policy with respect to their services and maintain a sufficient amount of insurance coverage for its liabilities to other Participants, including Subscribers and Relying Parties.

In particular, CSP, CA, CRA, (L)RA networks, SRA and other Zetes trusted services providers shall subscribe and bear the costs for own insurance coverage in order to cover their liabilities and duties in performance of their tasks.

ZETES TSP Qualified CA acting as CSP may request documentary evidence of such insurance coverage.

The liability of ZETES TSP Qualified CA towards the Subscriber or a Relying Party affected by the events listed in the section 9.2.1.1 may be limited according to the present CP.

9.2.1.1 Qualified certificates

As far as the issuance by ZETES TSP Qualified CA of Qualified Certificates is concerned, Article 13 of the Regulation (EU) No 910/2014 governs the liability of the CSP.

Following this provision, the CSP is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.

9.2.1.2 Certificates that cannot be considered as Qualified Certificates

Subject to any limitation of liability referred to in the CPS or in the present CP, the general rules on liability apply with regard to any damage caused to any entity or legal or natural person who reasonably relies on a Certificate issued by the CSP.

ZETES TSP Qualified CA explicitly declines all liability towards Relying Parties in all cases where non-Qualified Certificates (such as Normalized Certificates for authentication) are used in the context of applications allowing the use of such certificates for the generation of electronic signatures.

9.2.2 Other assets

ZETES TSP shall monitor on a regular basis that it maintains adequate resources to meet its obligations regarding the provision and use of its ZETES TSP Qualified CA offering under this Certification Practice Statement and elsewhere in its Agreements.

9.2.3 Insurance or warranty coverage for end-entities

Zetes benefits from insurance coverage covering ZETES TSP Qualified CA for public, product and professional liabilities.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Examples of confidential business information include:

- the Subscriber’s confidential information supplied to ZETES at the time of its subscription.
- the Subscriber’s or Relying Parties’ confidential information supplied to ZETES in support requests
- the private key(s) of Certificates

9.3.2 Information not within the scope of confidential information

For the avoidance of any doubt, the following information is NOT considered as confidential:

- the information published in a ZETES TSP Qualified CA issued Certificate
- the revocation records of a Certificate
- the Certification Practice Statement
- the Certificate Policy

9.3.3 Responsibility to protect confidential information

ZETES TSP and Subscriber Obligations of Confidentiality are described in the present CP.

ZETES TSP will keep confidential and not disclose the confidential information to any person save as expressly permitted by law or foreseen in the Agreement.

ZETES TSP will protect the confidential information against unauthorised disclosure by using the same degree of care as it takes to preserve and safeguard its own confidential information of a similar nature, being at least a reasonable degree of care and skill in accordance with the state-of-the-art.

9.4 Privacy of personal information

The ZETES TSP Qualified CA operates within the boundaries of the Belgian Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data. And conform the Law of 13 June 2005 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The ZETES TSP Qualified CA does not store any other personal data on certificates or on Subjects, other than the data, transferred to it and authorised by the RA. Without consent of the data subject or explicit authorization by law, personal data processed by the CSP will not be used for other purposes.

For the purpose of providing the Services under the Agreement between ZETES TSP and the Subscriber, the Subscriber is the data controller and ZETES TSP is the data processor. The Subscriber acknowledges that ZETES TSP processes any personal data in the frame of the Services under the Subscriber's responsibility, and that the legal obligations to inform data subjects (i.e. Subjects) and to notify national data protection authorities are the Subscriber's.

9.4.1 Privacy plan

9.4.1.1 ZETES TSP shall:

a) only process personal data on behalf of the Subscriber and according to the purposes communicated by and the instructions of the Subscriber and agreed to by the Subjects (see Section 4.1.2.2);

b) treat all personal data as confidential in accordance with Section 9.3, unless the Subscriber's determines otherwise;

c) take adequate technical and organisational measures ensuring the security of the processing of personal data in line with article 16 of the Act of 8 December 1992 on the protection of privacy with respect to the processing of personal data (hereinafter Personal Data Protection Act);

d) provide the Subscriber the opportunity to appropriately assess the adequacy of the implemented technical and organisational measures mentioned under (c);

e) notify the Subscriber as soon as possible of any request made by a data subject relating to the processing of his personal data;

f) duly assist the Subscriber in handling any reasonable request or complaint of a data subject relating to the processing of his personal data where whole or part of the processing is done by ZETES TSP;

g) refrain from transferring any personal data to sub-contractors or other third parties without the express permission of the Subscriber;

h) refrain from transferring any personal data outside the European Economic Area without the express permission of the Subscriber;

i) subject to the limitations set out elsewhere in this CP or in the Subscriber agreement, indemnify the Subscriber for any liability caused by processing personal data in breach of the provisions of this Section or its legal obligations as a data processor.

9.4.1.2 ZETES TSP warrants that:

a) the technical and organisational measures offer an appropriate level of protection in proportion to the risks involved against the accidental or unauthorised destruction, loss, alteration or access to personal data or any other form of unauthorised processing of personal data;

b) its personnel shall only have access to personal data insofar the access is necessary for performing their duties in providing the Services;

c) its personnel charged with the processing of personal data have been duly informed of the applicable obligations under the Personal Data Protection Act and their obligations under this Clause.

9.4.1.3 The Subscriber shall:

a) inform ZETES TSP in a clear and comprehensive manner of the intended purposes of the processing and provide clear and comprehensive directions regarding the extent to which ZETES TSP can access and use personal data;

b) indemnify ZETES TSP for any liability which is the direct result of processing personal data in line with the directions of the Subscriber.

9.4.2 Information treated as private

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.3 Information not deemed private

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.4 Responsibility to protect private information

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.5 Notice and consent to use private information

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.6 Disclosure pursuant to judicial or administrative process

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.7 Other information disclosure circumstances

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.5 Intellectual property rights

Any and all intellectual property rights (“IPR”) (including title, ownership rights, database rights, and any other intellectual property rights) in ZETES TSP Qualified CA’s Certificates offering, and documentation or other materials developed or supplied in connection with that offering, including any associated processes or any derivative works, are and will remain the sole and exclusive property of Zetes or its licensors.

No rights are granted by ZETES TSP in respect of ZETES TSP Qualified CA’s Certificates offering other than those expressly granted under this Certification Practice Statement or elsewhere in the Subscriber Agreement.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Zetes SA acting as CSP through its ZETES TSP Qualified CA issues X509 v3-compatible Certificates (ISO 9594-8).

ZETES TSP Qualified CA issues Certificates compliant with either ETSI EN 319 411 requirements. To this end, the CA publishes the elements supporting this statement of compliance.

ZETES TSP guarantees that all the requirements set out in the present CP (and indicated in the Certificate in accordance with Section 7) are complied with. It also assumes responsibility for ensuring such compliance and providing these services in accordance with the ZETES TSP Qualified CA CPS.

The sole guarantee provided by Zetes acting as CSP through ZETES TSP Qualified CA is that its procedures are implemented in accordance with the CPS and the verification procedures then in effect, and that all Certificates issued with a CP Object Identifier (OID) have been issued in accordance with the relevant provisions of the present CP, the verification procedures, and the CPS as applicable at the time of issuance. In addition, other warranties may be implied in the CP definition by operation of law.

9.6.2 RA representations and warranties

The RA needs under contractual obligation to comply with the CPS **[ref. 5]**, and with the RA relevant internal procedures.

Third party LRAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to, or which reasonably ought to be known to, the LRA or its agents;
- There are no errors in the information in the Certificate that were introduced by the LRA or its agents as a result of a failure to exercise reasonable care; and
- Their Certificates meet all material requirements of the CP/CPS.

Additional representations and warranties relevant to LRAs may be included in the Subscribers Agreements for specific Certificate Policies.

9.6.3 Subscriber and Subject representations and warranties

The Subscriber and Subject accept the “Certificate Terms and Conditions”.

The Subscriber agrees to the CPS and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the CPS and the present CP.

In particular, the Subject is liable towards Relying Parties for any use that is made of his / her SCD, including the keys or Certificate(s), unless (s)he can prove that (s)he has taken all the necessary measures for a timely revocation of his / her Certificate(s) when required.

9.6.4 Relying party representations and warranties

Examples of Relying Parties’ obligations and responsibilities include (without limitation):

- the successful performance of public key operations as a pre-condition for relying on a ZETES TSP Certificate
- the validation of a ZETES TSP Certificate by using the ZETES TSP Qualified CA’s Certificate Revocation Lists (CRLs)
- the immediate termination of any reliance on a ZETES TSP Certificate if it has been revoked or when it has expired

9.6.5 Representations and warranties of other participants

Zetes warrants that it operates the Secure Cryptographic Device Provisioning Services, the Dissemination and Repository Services, and the Revocation Management Services and the Revocation Status Information Services in conformity with the CPS.

9.7 Disclaimers of warranties

Except as expressly provided elsewhere in the CPS, the present CP and in the applicable legislation, ZETES TSP disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties.

ZETES TSP does not warrant "non repudiation" of any Certificate or message. ZETES TSP does not warrant any software.

9.8 Limitations of liability

Exclusion of Certain Elements of Damages

ZETES TSP Qualified CA explicitly declines all liability towards Subjects and Relying Parties in all cases where non-Qualified Certificates (such as Certificates with certificate profile: [NCP+]) are used in the context of applications allowing the use of such certificates for the generation of qualified electronic signatures.

Within the limit set by Belgian Law, in no event (except for fraud or wilful misconduct) will ZETES TSP be liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures;
- Any other damages beyond proven direct damages as described below.

In case of liability of ZETES TSP towards the Subscriber, the Subject or a Relying Party for proven direct damages, the liability of ZETES TSP towards any claimant is in any way limited to:

- paying damages amounting up to a maximum of 2500 € per transaction, for events where the Relying Party relies on that certificate:
  a) as regards the accuracy at the time of issuance of all information contained in the Qualified Certificate and as regards the fact that the Certificate contains all the details prescribed for a Qualified Certificate; or
  b) for assurance that at the time of the issuance of the Certificate, the signatory identified in the Qualified Certificate held the private key corresponding to the public key given or identified in the Certificate; or
  c) for assurance that the private key and the public key can be used in a complementary manner;

  and
- paying damages amounting up to a maximum of 10.000 € in total per Certificate that is underlying to the claim.

9.9 Indemnities

Zetes TSP acting as TSP assumes no financial responsibility for improperly used Certificates, CRLs, etc.

9.10 Term and termination of the present CP

9.10.1 Term

This CP and any amendments hereto shall become effective after publication in the Repository and in accordance with section 9.12.2 and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This shall remain in force until it is amended or replaced by a new version in accordance with this Section 9.10.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this CP will be communicated via the ZETES TSP web site upon termination. That communication will outline the provisions that may survive termination of this CP and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

9.11 Individual notices and communications with participants

All notices and other communications which may or are required to be given, served or sent pursuant to the CP or the CPS shall be in writing and shall be sent, except provided explicitly in the CP, either by (i) registered mail, return receipt requested, postage prepaid, (ii) an internationally recognised “overnight” or express courier service, (iii) hand delivery (iv) facsimile transmission, deemed received upon actual delivery or completed facsimile, or (v) an electronic document or electronic message with an advanced electronic signature or a qualified electronic signature and be addressed to the contact information mentioned in chapter 1.5.2.

9.12 Amendments to the present CP

9.12.1 Procedure for amendment

ZETES TSP acting as TSP is responsible via its Policy Management Authority (PMA) for approval and changes of the CP.

The only changes that the PMA may make to these CP specifications without notification are minor changes that do not affect the assurance level of this CP, e.g., editorial or typographical corrections, or changes to the contact details.

Errors, updates, or suggested changes to this document shall be communicated as identified in section 1.5.4. Such communication must include a description of the change, a change justification, and contact information of the person requesting the change.

The PMA shall accept, modify or reject the proposed change after completion of a review phase.

9.12.2 Notification mechanism and period

All changes to the CPS under consideration by the PMA shall be disseminated to interested parties for a period of minimum 10 days. The date of issuance and the effective date are indicated on the title page of the present CPS. The effective date will be at least 2 days later than the date of publication.

9.12.3 Circumstances under which OID must be changed

Changes to this document that are limited to editorial corrections and typographical corrections or that do not entail significant effects for the relying parties, subscribers or subjects, are considered minor changes. Minor changes result in the update of the minor version number of the document but do not require a new OID. Major changes are changes that have a significant impact on the acceptance of the certificates and/or on the intended use of the certificates and will require an update of the major version number of the document and a change of the OID. Where applicable the OID shall be encoded in the certificate, so that relying parties and subjects can clearly identify the correct policy for said certificate.

9.13 Dispute resolution provisions

All disputes associated with the CPS will be resolved according to the Belgian laws.

9.14 Governing law

The Belgian laws shall govern the enforceability, construction, interpretation, and validity of the present CP (without giving effect to any conflict of law provision that would cause the application of other laws).

9.15 Compliance with applicable law

The CPS and provision of CA certification services are compliant to relevant and applicable laws of Belgium (including the directly applicable Regulation (EU) No 910/2014).

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

Not applicable.

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