# ZETES TSP QUALIFIED CA

## COMMON CERTIFICATE POLICY FOR OVB-OBFG

*Common Certificate Policy*

*for certificates issued on behalf of*

*OVB-OBFG*

| | | | |
|---|---|---|---|
| **Publication date :** | **27/03/2017** | | |
| **Effective date :** | **29/03/2017** | | |
| **Document OID :** | **1.3.6.1.4.1.47718.2.1.2.2.1.10 (NCP+)**<br>**1.3.6.1.4.1.47718.2.1.2.2.3.10 (QCP-n-qscd)** | | |
| **Version :** | **1.0** | **23/03/2017** | **PMA approved** |

# Table of Content



  

  

  

# Figures



# Tables



  

# ABOUT THIS DOCUMENT

## Scope

The present document is a Certificate Policy (CP) for certificates issued by the ZETES TSP Qualified CA on behalf of a third party.

The policy applies to the issuance of Normalized Certificates and of Qualified Certificates meeting the requirements of Regulation (EU) No 910/2014 **[ref. 1]** under the Certification Practices Statement (CPS) for the ZETES TSP Qualified CA **[ref. 2]**.

## Intellectual Property Rights



## Document Version History

| Version | Publication Date | Effective Date | Information about this Version |
|---|---|---|---|
| **1.0** | 27/03/2017 | 29/03/2017 | first publication ---------- |

# ABOUT ZETES

### About Zetes SA

Founded in 1984, Zetes is an international group highly specialised in identification and mobility solutions. Our head office is located in Brussels and our team is made up of more than 1,100 experts spread across 20 countries in the EMEA region.

ZETES SA is a private enterprise incorporated in Belgium. Zetes SA is active in the areas of identification documents, travel documents, biometrics and trust services including the issuance of certificates.

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

Zetes delivers people authentication solutions to governments, administrative units and public institutions, based on technologies: biometrics, AFIS and smartcards. People authentication is used in the areas of people registration, mass enrolment, data centralisation and validation, secure document production and electronic voting.

Zetes is registered as follows:

| Dutch language | French language | English language |
|---|---|---|
| **Zetes NV** | **Zetes SA** | **Zetes SA** |
| Straatsburgstraat 3<br>1130 Brussel<br>België<br>BTW BE 0408 425 626 | Rue de Strasbourg 3<br>1130 Bruxelles<br>Belgique<br>TVA BE 0408 425 626 | Rue de Strasbourg 3<br>1130 Brussels<br>Belgium<br>VAT BE 0408 425 626 |

Under Belgian law, NV (*Dutch* Naamloze Vennootschap) and SA (*French* Société Anonyme) are equivalent terms.

### About ZETES TSP business unit

In 2016, Zetes Trust Services Provider (ZETES TSP) was established as an operational business unit within Zetes SA to provide certificate services and trust services for governments, the financial sector and private organisations.

ZETES TSP operates its own PKI infrastructure and acts as a Trusted Service Provider (TSP) as defined in the Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. To this regard, ZETES TSP Qualified CA is supervised by Be.Sign, the Belgian Supervisory Body and is listed in the Belgian Trusted List of Qualified TSP issuing Qualified Certificates.

# 1 INTRODUCTION

## 1.1 Overview

**The present document is a Certificate Policy (CP)**

The ZETES TSP Qualified CA issues Qualified Certificates and Normalized Certificates to natural persons. ZETES TSP is acting as the Certification Service Provider (CSP).

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

These organisations are collectively referred to as OVB-OBFG 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 and/or OBFG 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 Certification Practice Statement (CPS) **[ref. 2]**,
- the present ZETES TSP Certificate Policy (CP),
- the relevant ZETES TSP Certificate Terms and Conditions (CTC) **[ref. 3]**.

The present document states the policies applicable to these certificates in terms of certificate profiles, applicability and management lifecycles. It focuses on the role and responsibilities of the PKI participants and defines the procedures for Subject enrolment, certificates issuance, revocation etc.

ZETES TSP has final and overall responsibility for the provision of the ZETES (Qualified) Certificates offering, namely:

- the provision service for the Secure Cryptographic Device,
- the personalisation and delivery service for the Secure Cryptographic Device,
- the Certificate generation services through the ZETES TSP Certification Authority (CA),
- the Registration Management Services through the ZETES TSP Registration Authority network of subordinate and local RAs,
- the Suspension and Revocation Management Services through the ZETES TSP Suspension and Revocation Authority network of subordinate and local SRAs,
- the Revocation Status Information Service (providing certificate validity status information through publication of Certificate Revocation Lists and/or through OCSP services),
- the Dissemination Services.

Every certificate issued by the ZETES TSP Qualified CA contains a Certificate Policy OID corresponding to the type and the assurance level of the Certificate:

| Policy | Policy Identifier | 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. |
| 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. |

Such certificates may be complemented by an OID identifying their domain of issuance and authorised Subscriber where relevant, such as it is the case for OVB-OBFG (see chapter 7).

### 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.

### Old and New Terminology used for Secure Cryptographic Devices

This documents uses the term "Secure Cryptographic Device" to refer to the cryptographic device which is provided to the Subject. 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:

- the device allows to generate 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 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.
- Specifically, the Secure Cryptographic Device must have 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.

### 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'. 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** | |
|---|---|
| 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(10)} |

| **ZETES TSP Qualified CA - QCP-n-qscd certificates for OVB-OBFG** | |
|---|---|
| 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(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.<br>For this CP, the Subscriber is the OVB-OBFG. |
| **Subjects** | Natural persons whose identity or identifier is encoded in the end user certificate issued by a CA. A Subject adheres to a Subscriber.<br>For this CP, the Subject is a lawyer who is a registered member of OVB or OBFG, 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 |
| **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 | For this CP, the SUB-RAs are the OVB and OBFG.<br>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. |
| **L-RA** - Local Registration Authorities | The task of L-RA is performed by the local bar associations (NL "*balies" / FR "barreaux"*) of OVB and OBFG.<br>The local representative of the SUB-RA. The L-RA performs the front-office registration tasks and first-line vetting of Subjects. |
| **SRA** - Suspension and Revocation Authority | The entity representing the overall organisation of suspension and revocation authority bodies. Has supervising authority over the C-SRA, SUB-SRAs and L-SRAs, authenticates suspend/revocation requests from the SUB-SRAs. |
| **C-SRA** - Central Suspension and Revocation Authority | The central infrastructure at ZETES TSP for processing suspension and revocation requests, dissemination of certificate status information. It is the only part of the SRA that is in direct contact with the CA. |
| **SUB-SRA -** Subordinate Suspension and Revocation Authority | The authority for the registration or initiation of suspension and revocation requests for a specific Subscriber or group of Subscribers. The SUB-SRA is usually associated with or part of the Subscriber.<br>For this CP, the SUB-SRA are the OVB and OBFG. |
| **L-SRA** - Local Suspension and Revocation Authority | The local representative of the SUB-SRA. The L-SRA performs the front-office request procedure and vetting procedure for a Subject requesting suspension or revocation of the Subject's certificate.<br>For this CP, the task of L-SRA is performed by the local bar associations (balies / barreaux) of OVB and OBFG. |
| **Publication and Repository Services** | Online publication of documents such as Certification Practice Statements, Certificate Policies, Certificate Terms and Conditions, certificate validation data such as root certificates, certificate revocation lists, etc. |
| **Secure Cryptographic Device** | The Secure Cryptographic Device is a PKI smartcard that meets the requirements for EU Qualified Electronic Signature, i.e. the Secure Cryptographic |

| | |
|---|---|
| | Device is a Qualified Signature Creation Device (QSCD). |
| **Secure Cryptographic Device - Provisioning Services** | ZETES TSP is responsible for supplying the Secure Cryptographic Device to the Subjects. |
| **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.<br><br>Card Delivery Services 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.

This is illustrated by the following diagram:

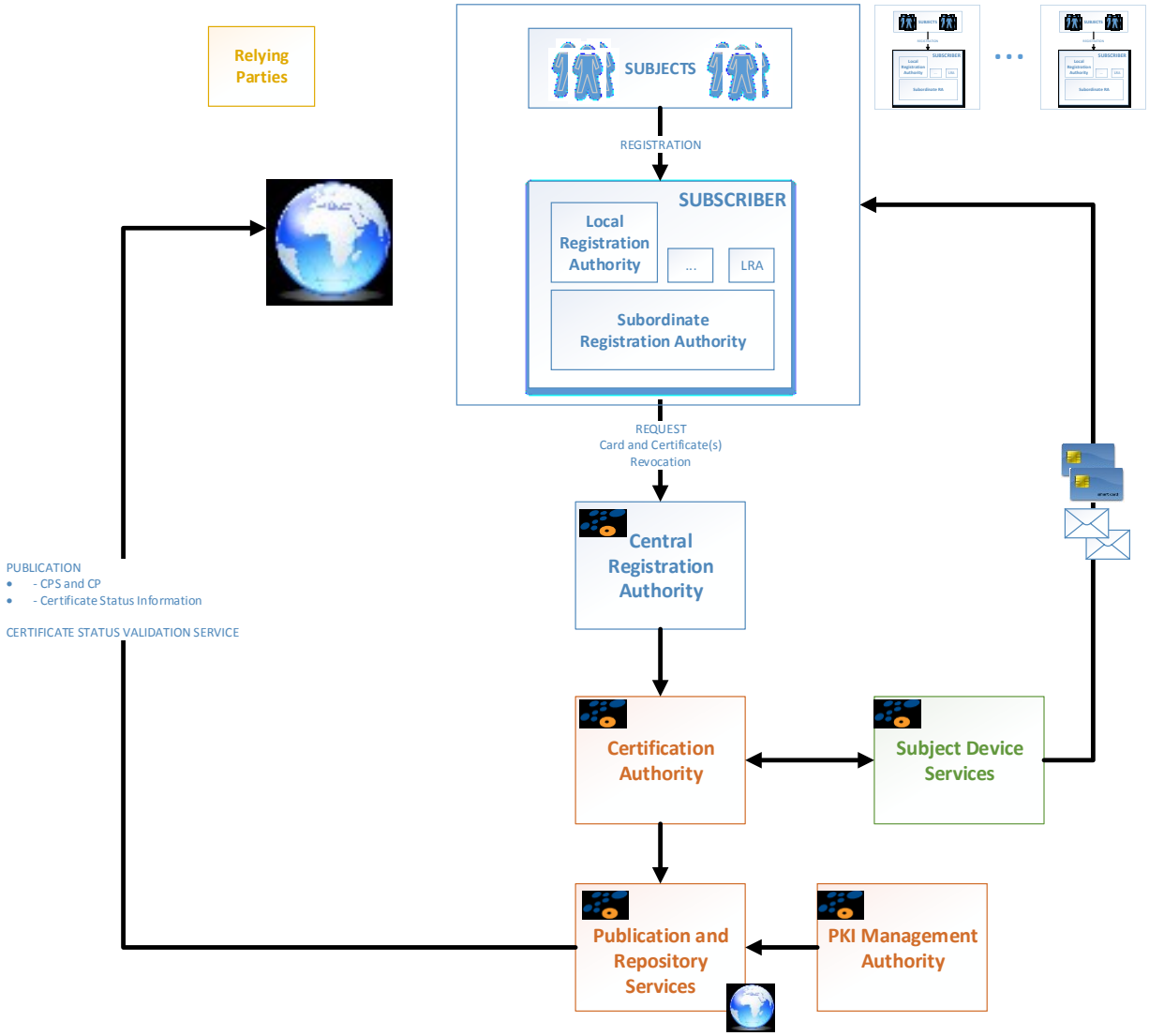


**Figure 1 Diagram of the PKI participants**

### 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

The following schematic illustrates the 2-level CA hierarchy for issuing Normalized Certificates and Qualified Certificates to Subjects.

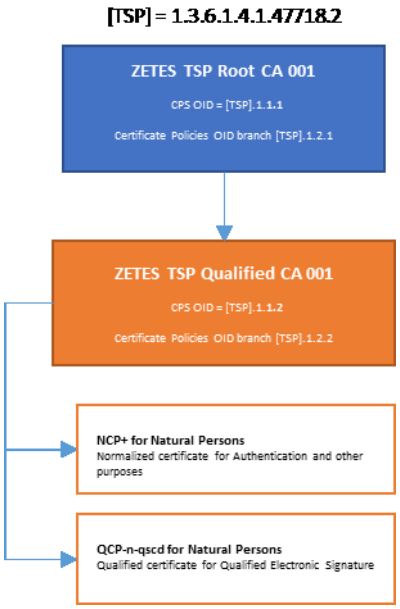


**Figure 2 CA and certificates**

### 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 RA also includes a supervisory body to supervise and audit the various other constituent parts of the RA.

This is illustrated below:

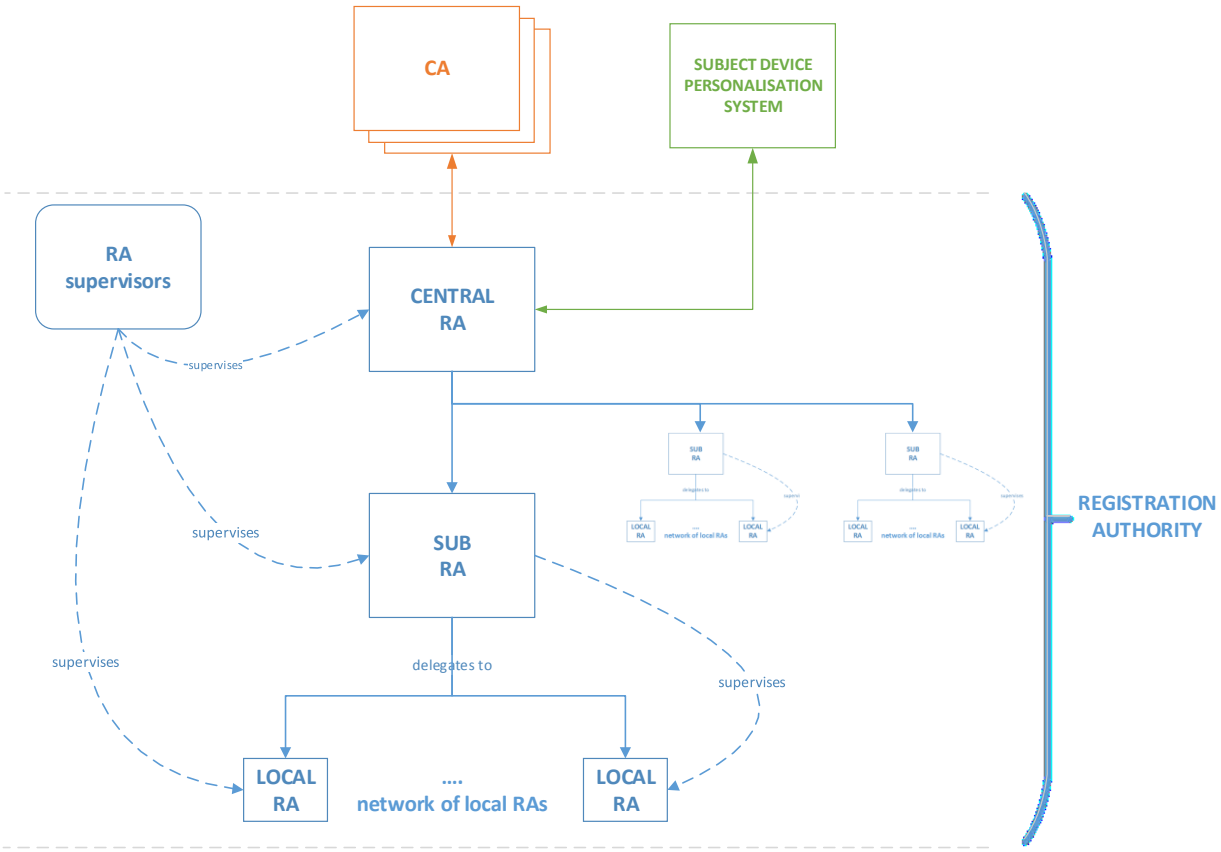


**Figure 3 Registration Authority entities**

### 1.3.2.2 Central Registration Authority (C-RA)

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

- process certificate requests originating from Subordinate RAs
- authenticate and validate the Subordinate RA and the certificate request itself
- act upon the result of this validation and, if approved,
    - select the appropriate Certificate Profile
    - interact with the card personalisation process for key generation
    - submit a certificate request to the appropriate CA
    - retrieve the certificate from the CA
    - interact with the card personalisation process for encoding the certificate

The infrastructure for the Central RA is closely integrated with the Card Personalisation and Delivery Service:

- certificate requests are implicitly part of card personalisation requests
- a request for a card can lead to more than one certificate request

- the vetting process for a card personalisation request implicitly covers the vetting process for the associated certificate requests
- the RA is integrated with the card personalisation / chip encoding process
    - the Subject's keys are generated in the embedded chip of the Secure Cryptographic Device (card)
    - the interaction with the CA for obtaining the certificate(s) for a card is coordinated with the sequence of the card personalisation process

The Central Registration Authority (Central RA) interacts with the CA to:

- Send certificate creation requests;
- Retrieve the certificates issued by the CA;
- Send certificate revocation requests;
- Retrieve CRLs issued by the CA

The Central RA does not interact directly with a Local RA. The Central RA does not interact directly with a Subject.

#### 1.3.2.3 Subordinate Registration Authorities (SUB-RA)

The Subordinate Registration Authorities are the entities which are tasked with the organisation and the coordination of the registration process and the certificate delivery process for a specific group of Subjects.

In the case of the present CP, OVB and OBFG 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.

#### 1.3.2.4 Local Registration Authorities (L-RA)

The Local RAs are the entities that are responsible for the actual registration of the Subject for whom the certificates are intended. The L-RA offices are the point of contact for the Subjects for in-person registration, for handover and post-issuance update of the Secure Cryptographic Device to the Subjects.

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 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*

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)

The Subscriber is the entity, composed of the organizations OVB-OBFG, who enters into a contractual agreement with Zetes for the purpose of issuing certificates to Subjects. A Subscriber must have a contractual agreement, membership agreement or some form of legal authority over the Subjects it represents.

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

A 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.

In the case of the present CP, OVB-OBFG is the Subscriber. These organizations have signed a Subscriber Agreement with ZETES. In addition, the CPS, the present CP and CTC are an integral part of the Subscriber agreement.

#### 1.3.3.2 Subjects (natural persons)

For the context of this Certificate Policy, the Subject can be:

- a lawyer who is a registered member of OVB or OBFG,
- 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 (Qualified) Certificate by verifying the signature of a Subject. These 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 exported in clear text form. Some Secure Cryptographic Devices provide additional controls to prevent use of the private key before the Secure Cryptographic Device or a specific key pair on the Secure Cryptographic Device have been explicitly accepted by the Subject. See also chapter 3.2.1 and chapter 6.2.8 to 6.2.9 for related topics.

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 operating the Dissemination Services (publication of Certification Practice Statement, Certificate Policy, Certificate 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, Certificate 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.

Revocation of a Certificate can be requested by the Subscriber, by the Subject to which the Certificate is issued, as well as by ZETES TSP in its role as Certification Service Provider as ruled by the present Certification Practice Statement.

### 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 [2].

## 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, 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<br>1130 HAREN<br>BELGIË | 3, rue de Strasbourg<br>1130 HAEREN<br>BELGIQUE |
| **Telephone:** | 0032 2 728 37 11 | |
| **Fax:** | 0032 2 728 37 52 | |
| **Web site:** | http://tsp.zetes.com | |

### 1.5.3 Person determining CP 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 Certification Practice Statement.

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

Errors, updates, or suggested changes to this Certification Practice Statement 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 |
| DN | Distinguished Name |
| CTC | Certificate Terms and Conditions |
| 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 made available by the CA to Subscribers and Relying Parties. The CRL is updated after each Certificate revocation process. The CRL does not necessarily contain identifiers of revoked Certificates that are past their validity date (that is, expired). |
| 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.<br><br>The Regulation distinguishes between Qualified Certificates for different purposes: electronic signature, electronic seals, or website authentication. |

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

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

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

The same information is also 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 as follows:

| | |
|---|---|
| **http://tsp.zetes.com**<br>**https://tsp.zetes.com** | This URL refers to the welcome page of the web site for ZETES TSP.<br>This web site provides:<br>• general information about Zetes SA and the ZETES TSP business unit<br>• announcements and notifications<br>• a section with technical support and documentation and software downloads for users of the cards and/or certificates that are issued by ZETES TSP<br>• a section with user friendly web pages for downloading documents such as the terms and conditions, certificate policies, etc.<br>• a section with user friendly web pages for downloading CA certificates and certificate revocation lists (the URLs for these download pages are listed further down in this table)<br>• a contact page |
| **https://repository.tsp.zetes.com**<br>**https://pds.tsp.zetes.com** | These URL refers directly to the page for downloading documents such as<br>• CPS - Certification Practice Statements,<br>• CP -Certificate Policies,<br>• CTC - Certificate Terms and Conditions,<br>• PDS - PKI Disclosure Statements<br>• etc. |
| **http://crt.tsp.zetes.com** | This URL refers to<br>1. a web page for manual interactive download of CA certificates<br>2. a server for automated direct download of CA certificates (the direct download link is encoded in the certificates) |
| **http://crl.tsp.zetes.com** | This URL refers to<br>1. a web page for manual interactive download of ARL and CRL<br>2. a server for automated direct download of ARL and CRL (the direct download link is encoded in the certificates) |
| **http://ocsp.tsp.zetes.com** | This URL refers to the OCSP service for immediate online certificate status checks. The OCSP service is synchronised with the latest CRL to provide answers and checks the expiration before the revocation. |

## 2.2 Publication of certification information

### Availability

Availability of the document repository is designed to exceed 99.0% of business hours - defined as 24 hours per day, seven days per week, excluding planned maintenance periods.

Planned maintenance periods 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.

### 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 Certificate Policy and 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, as a matter of policy, publishes its CA certificates in a public certificate repository. This policy is clearly stated in the Certificate Policy and in the contractual agreement with the Subscriber (if applicable).

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

Certificate status information is made available in two formats:

- as downloadable ARLs, CRLs and delta-CRLs
- as OCSP service

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

The CRLs or delta-CRLS are renewed when certificates have been revoked or when the CRL or delta-CRL is about to expire. The OCSP service is synchronised with the latest CRL.

Certificate status information in CRLs and the OCSP service is updated until all certificates that that were issued by the respective CA have expired. For Qualified Certificates, the certificate status information will remain available beyond the validity period of the certificate, until the issuing CA certificate has expired.

More information is available in section 4.10.

## 2.3 Time or frequency of publication

### Publication of CA certificates in a repository

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

### Certificate Status Information

The CRL is created either every 24 hours. A delta-CRL is created ever hour.

CRLs and delta-CRLs are published in the repository immediately following creation, and will be available for download within 20 minutes after creation.

The OCSP service is immediately synchronised with the latest CRL when that CRL is published.

### Publication of terms and conditions, CSP, etc.

Updates to the Certificate Policy, Certification Practice Statement, Certificate Terms and Conditions, and other public documents are 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 will take reasonable measures to protect and prevent against abuse of the repositories and the OCSP service and will strive to give all parties equal and unhindered access.

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**).

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).

| **Naming convention ETSI EN 319 411 part 1 General Requirements and ETSI EN 319 411 part 2 for EU Qualified Certificates issued to Natural Persons** | |
|---|---|
| **Certificate Attribute** | **Description** |
| **serialNumber** | **Subject serial number or identifier, t**his is a unique identifier (UUID) as assigned by OVB-OBFG. |
| **title** | **official title of the Subject** as assigned by OVB-OBFG |
| **givenName** | **Official given name(s) of the Subject** as validated by the SUB-RA/L-RA.<br>space (" ") separated full-form concatenation of given names, identical to how it is stated on 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.<br>Space (" ") separated full-form concatenation of surnames, identical to how it is stated on the identity document that was used to register the Subject |
| **commonName** | **Official name or calling name of the Subject + indication of the intended purpose for this certificate**<br>The certificate will only contain one instance of commonName. The commonName is intended for a user friendly representation of the certificate holder's name.<br>Space (" ") separated short-form concatenation of given name(s) and surname(s) and information identifying the purpose or use context of the certificates. |
| **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,**<br>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.<br>For the context of this Certificate Policy, the **organizationName** is one of the following: |

| | |
|---|---|
| | • **"Orde van Vlaamse Balies (KBO 267.393.267)"**<br>• **"Ordre des Barreaux Francophones et Germanophone de Belgique (BCE 850.260.032)"** |
| **organizational Unit** | **The certificate may contain zero, one or more OU fields.**<br>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

**Proof of Possession of Private Key for Secure Cryptographic Devices**

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

The Secure Cryptographic Device is selected by Zetes.

The Secure Cryptographic Device used for certificates for natural persons complies with the technical standards and certification requirements as defined for Qualified Secure Signature Creation Device.

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.

Specifically, the Secure Cryptographic Device must have 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 419 211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application.

In practice, the device is a smartcard or a device with an embedded PKI chip with the following features:

- cryptographic key pairs are generated inside the chip
- private keys cannot be extracted from the chip
- public keys can be extracted, in some cases at any time after key generation, in other cases only immediately following the key generation process and within the same session
- the chip requires a PIN or biometric Match on Card (e.g. fingerprint verification) to use the key pair for cryptographic operations such as authentication or electronic signature,
- optionally, the chip may provide additional control mechanisms to prevent any use of a private key prior to explicit consent of the Subject.

The key generation process complies with the ETSI EN 319 411 parts 1, 2 as applicable for the type of device, purpose and certificate.

This key generation process is always performed under controlled conditions, in a secure environment and under the supervision of authorized personnel. The CA only accepts authenticated certificate requests that originate from inside this controlled environment.

The key generation process for the Secure Cryptographic Device as well as the certificate request generation process is an integral part of the personalisation process of the Secure Cryptographic Device. Initialization, pre-issuance personalisation and post-issuance personalisation of the Secure Cryptographic Device is performed on behalf of ZETES TSP and under supervision of Zetes TSP in a secure environment and under controlled conditions. These processes involve participation of one more other actors such as the Secure Cryptographic Device Provisioning party, the sub-RA and the Subject.

The secure environment includes:

- the card personalisation facility of Zetes,

- the card & key management system operated by Zetes ,
- the infrastructure for post-issuance personalisation
- the security mechanisms of the Secure Cryptographic Device
- the virtual environment of keys and codes used for authentication, authorization and protecting card personalisation operations and the physical infrastructure that is used to protect these keys and codes

The secure environment is therefore the combination of a secure physical environment, a secure virtual environment and the processes and procedures that are applied in those environments.

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.

### 3.2.2 Authentication of organization identity

**Organization acting as a Subscriber**

It is reminded that ZETES TSP Qualified CA does not issue certificates to organizations, but to natural persons only.

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 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 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

**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 authentication procedure to verify the identity of a Subject and to verify the Subject's association with the Subscriber, complies with the requirements specified in ETSI EN 319 411-1 for the following certificate profile: [NCP+], and as specified in ETSI EN 319-411-2 for the following certificate profile [QCP-n-qscd].

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

Nevertheless, Subjects must explicitly register for a new Secure Cryptographic Device including certificates or for new certificates. This is either initiated on invitation by the L-RA or on the Subject's own initiative.

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

- online
- by e-mail
- in person at the Local RA office with which the Subject is associated.

The second step of the registration process is the handover of the Secure Subject Device and/or the certificates to the Subject. This step can only be done in person at the Local RA office. The L-RA operator checks the Subject's identity document again to finalize the registration process and before the handover.

**Registration Step 1 by means of online Registration:**

Subjects who are holder of a Belgian electronic Identity Card or a Belgian electronic Residence Permit Card can use the online registration portal. Subjects have to authenticate (log on) with their eID card, which implies possession of the eID card and knowledge of the eID PIN code.

The procedure meets the requirements for a remote online registration and authentication method, using electronic identification means, for which a physical presence of the Subject was ensured and meets the requirements as set out in Regulation (EU) n° 910/2014 Article 8 level High or Substantial.

**Registration Step 1 by e-mail or in person:**

Subjects not registering online with the Belgian eID card and eID PIN code must in all cases provide proof of a valid and authentic identity document (national identity card, residence permit, passport, etc.) to the Local RA operator.

Alternatively, the registration procedure can be performed in person at the Local RA office with which the Subject is associated and present a valid and authentic identity document.

**Registration Step 2:**

In all cases, the Subject will have to appear in person in front of an authorized operator of the Local RA and present the valid and authentic identity document (national identity card, residence permit, passport, etc.) to the Local RA operator to conclude the registration process and before the handover of a new Secure Cryptographic Device with certificates and/or the update of an existing Secure Cryptographic Device with new certificates.

The Local RA operator validates the authenticity of the presented documents and checks that the individual is the genuine holder of the presented documents according to rules defined by ZETES TSP internal instructions and - optionally - additional rules defined by the Subordinate RA and/or the Subscriber.

**Entitlement check:**

In addition to identifying and authenticating the Subject, the SUB-RA / L-RA validates the request and checks the Subject's entitlements: i.e. the Subject is a registered Member of the OVB or OBFG, is a registered staff member, …

**Authentication of Professional Attributes or Membership Attributes**

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

OVB or OBFG 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 as the Subscriber and OVB or OBFG 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

OBVB-OBFG 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 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.

### 3.3.2 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 or OBFG as the Subordinate RA and as the representative of the Bar Associations (also the Local RAs)
- OVB-OBFG 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 authenticated by means of an identity check in the physical presence of the Subject if the revocation request is lodged in an L-RA office, or by means of validation of control questions 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.

ZETES TSP provides the infrastructure and the operational resources for the Central RA. ZETES TSP also provides supervision, support for and auditing for all the entities of the RA. Some services of the RA such as Subordinate RAs and their Local RAs are performed by the Subscriber.

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

The Central RA relies on the enrolment process performed by OVB and OBFG as the Subordinate RAs. The Subordinate RAs delegate the enrolment process to their local Bar Associations as the 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.

#### 4.1.2.2 Enrolment of Subjects

**The Subject Agreement**

The Subject is supplied with the following information which together constitutes the Subject Agreement:

- 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 when 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 signed receipt is considered the formal acceptance by the Subject of the Subject Agreement whereby the Subject accepts

- his 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 counting from the date of the issued certificate 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 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 or 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.

The Central RA or 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 Central 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. 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.

#### Compliance with Standards

Unless explicitly stated otherwise, the processes are compliant with the relevant technical standards ETSI EN 319 411-1 for all Certificates and ETSI EN 319 411-2 for Qualified Certificates.

### 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 may play a role in the enrolment process of Subjects (or in the Subject certificate revocation process), e.g. relating to professional attributes, membership attributes, entitlement to request a certificate mentioning the organisation of the Subscriber, etc.

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 counting from the date of the issued certificate 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 Officers 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. The CA, the Central RA and the personalisation and management system are integrated systems and communicate over closed network connections. The CA will only process requests that originate from a trusted system which is internal to ZETES TSP.

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

- Does the request originate from a trusted source
- The CA will check the requester's authorization for the type of request and refuse requests that pertain to certificate profiles for which the requester is not authorized.
- The CA also matches the certificate request against a pre-defined certificate profile. The variable information in the request must match with the template and rule set of the certificate profile.
- The CA will add non-variable and variable information to the certificate, as defined in the certificate profile.

### 4.3.2 Notification of issuance of certificate

If the certificate is issued as part of the personalisation process of the Secure Cryptographic Device, the Subject receives a notification as part of the delivery procedure of the Secure Cryptographic Device. Alternatively, the Subject was informed beforehand of the delivery period for the Secure Cryptographic Device.

If the certificate is issued for an already existing Secure Cryptographic Device, the Subject receives an invitation to go to the Local RA at a specific date or is given a specified period within which to go to the Local RA.

One month before the expiration of its certificate, the Subject is informed that the certificate is about to expire.

## 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 the privacy policy
- the information letter including instructions and Activation Data
- a receipt to confirm the handover of the new Secure Subject Device to the Subject (if applicable)
- a declaration of acceptance by the Subject of the new certificate(s)
- declaration of acceptance by the Subject of the Certificate Terms and Conditions

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 Local SRA or the Subordinate SRA must request revocation of the certificates
- the Central 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 Local RA officer will provide the Subject 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

Not applicable for Subject certificates. The ZETES TSP Qualified CA does not renew certificates, i.e. does not issue new 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

Certificate re-keying for Subject certificates involves

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

Certificate re-keying is allowed only if the conditions described in chapter 3.2.1.

## 4.8 Certificate modification

Not applicable for Subject certificates. The ZETES TSP Qualified CA does not modify certificates, i.e. does not issue modified 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,

- ad-hoc as specified in applicable Certificate Policy.

### 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 an authorized Local SRA or via an automated procedure under control of the SRA. The procedures and access points for requesting revocation are described in the Subject Agreement.

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

| CHANNEL | SUBSCRIBER AUTHENTICATION MECHANISMS |
|---|---|
| **SUB-RA/SRA internal membership register management system** | **identification**<br>• a combination of name, organization and role<br><br>**authentication mechanisms**<br>• 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 are 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 (if applicable)

The ZETES TSP Qualified CA issues CRLs and delta-CRLs at pre-defined intervals or ad hoc when needed.

The CRL and delta-CRL are signed and time-marked by the CA. The renewal period is 1 day for CRL and 1 hour for delta-CRL.

### 4.9.8 Maximum latency for CRLs (if applicable)

ZETES TSP will make best effort to update the certificate status information not later than 1 hour after 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

### 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

http://crt.tsp.zetes.com

http://crl.tsp.zetes.com

### 4.9.12 Special requirements re 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 Limits on suspension period

Not applicable.

## 4.10 Certificate status services

### 4.10.1 Operational characteristics

The ZETES TSP Qualified CA provides 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 (full and delta)
- Online Certificate Status Protocol service, open for unsigned requests

### 4.10.2 Service availability

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

OCSP service availability is designed to 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 [2].

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.

# 6 TECHNICAL SECURITY CONTROLS

For description of the technical security controls (including secure key management) applicable to the ZETES CPS (CA, RA and other PKI components services), refer to section 6 of the CPS [2].

## 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

The ZETES TSP Qualified CA has a network connection to internal systems of ZETES TSP for generating keys for Secure Cryptographic Devices that are personalised by Zetes on behalf of ZETES TSP.

Certificate requests (that include the public key of the requester) are transferred by means of a trusted network connection between the environment for the initial personalisation or the post-issuance personalisation of Secure Cryptographic Devices and the environment for the CA.

Two methods are supported:

- the public key is extracted from the Secure Cryptographic Devices just in time, as part of the initial or post-issuance personalisation process for the Secure Cryptographic Device, i.e. with the Secure Cryptographic Device present
- the public key was extracted from the Secure Cryptographic Devices and stored in a database, from which it can be read without he Secure Cryptographic Device present

The actual method depends on the capabilities of the Secure Cryptographic Device that is used and on the preferred optimization of the (initial/post-issuance) personalisation process for the Secure Cryptographic Device.

### 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 are published on a secure web site:

https://repository.tsp.zetes.com

Relying Parties can 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 is 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

The current PKI infrastructure for the ZETES TSP Qualified CA uses the following algorithms and key sizes:

| | | |
|---|---|---|
| Secure Cryptographic Devices* | RSA2048 | generated and used on the SCD |
| CA | RSA4096 | generated and used on HSM |
| OCSP service | RSA2048 | generated and used on HSM |

** Secure Cryptographic Device for Subjects and for RA/SRA operators and CA operators*

All certificates are 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

Public key parameters are generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Public key parameters shall be generated and tested in accordance with the FIPS 186-2 standard which ensures the quality of the key material.

The following parameters are used depending on the algorithm family:

RSA:

- the HSM is used in FIPS mode
- key generation relies on the deterministic random number generator that is compliant with FIPS 186-2 Appendix 3.1,
- public exponent '010001'

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

ZETES TSP ensures 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 the document Certificate Profiles, below is an overview:

Key usage for user certificates for authentication purposes: digitalSignature

Key usage for user certificates for electronic signatures: nonRepudiation

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic module standards and controls

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).

### 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. The embedded microchip protects private keys and other security related information against hacks.

### 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.

The Secure Cryptographic Device may also provide a security feature (known as a "Transport PIN") to prevent use of the private key prior to explicit commissioning of the key by the Subject, typically as part of the initial handover procedure of the Secure Cryptographic Device or as part of a post-issuance update procedure e.g. for certificate re-keying or for adding new keys and certificates to a Secure Cryptographic Device already in use.

### 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 maintains 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 will not issue certificates that exceed the certificate expiration date of the CA certificate.

The key usage period of a CA key is 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 [2].

## 6.6 Life cycle technical controls

ZETES TSP ensures life cycle technical controls described in the CPS [2].

## 6.7 Network security controls

ZETES TSP ensures network security controls described in the CPS [2].

## 6.8 Time-stamping

Not applicable.

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificate profiles

This Certificate Policy applies to NCP+ certificates and QCP-n-qscd certificates issued on behalf of OVB-OBFG as Subscriber.

Applications rely on standardized and interoperable certificate profiles, in particular applications that are used for electronic signature or authentication in open environments.

The certificates issued by the Zetes TSCP 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.

The Certification Practice Statements are published in the Zetes TSP repository on https://repository.tsp.zetes.com.

### 7.1.2 Certificate Profile for Authentication of the Certificate Holder

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 authentication purposes for the Subject, e.g. for as SSL/TLS client authentication.

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.

The key pairs are RSA2048. The certificate validity period may vary but is maximum 36 months.

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

| | | | | |
|---|---|---|---|---|
| **certificate profile**<br>**ZETES TSP NCP+ certificate for natural persons for the Subscriber OVB-OBFG**<br>**certificate policy OID: 1.3.6.1.4.1.47718.2.1.2.2.1.10**<br>**certificate profile OID: 1.3.6.1.4.1.47718.2.1.3.2.1.10**<br>version 1.0 | | | | |
| **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** |
| | **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**<br>This is a unique identifier (UUID) as assigned by OVB-OBFG. |
| | **title** | - | MD | **title of the Subject** *as assigned by the SUB-RA/LRA*<br>Dutch: "**advocaat**"<br>"**staff member**"<br>French : „**avocat**"<br>„**staff member**"<br>German : „**Rechtsanwalt**"<br>„**staff member**" |
| | **givenName** | - | MD | **official given name(s) of the Subject**<br>space (" ") separated full-form concatenation of given names, identical to how it is stated on the breeder document that was used to register the Subject |
| | **surname** | - | MD | **official surname(s) of the Subject**<br>space (" ") separated full-form concatenation of surnames, identical to how it is stated on the breeder document that was used to register the Subject |
| | **commonName** | - | MD | **the name of the Subject as assigned by the SUB-RA/LRA and an indication of the intended purpose for this certificate**<br>The format is a space separated concatenation of :<br>• the label "**AUT**" identifying the purpose of the certificate<br>• short-form surname of the Subject<br>• short-form given name of the Subject<br>• the title of the Subject in parentheses e.g. (advocaat) |
| | **countryName** | - | MD | **nationality of the Subject**<br>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<br>"**Orde van Vlaamse Balies (KBO 267.393.267 )**"<br>or<br>"**Ordre des Barreaux Francophones et Germanophone de Belgique (BCE 850.260.032)**" |
| | **organizationalUnitName** | - | OD | **T**he 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**<br>{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) **calssuers**(2)} |
| | **accessLocation** | - | MS | **http://crt.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crt**<br>*(001 is the 3-digit serialNumber of the ZETES TSP QUALIFIEDCA 001)* |
| | **accessMethod** | - | MS | **OID 1.3.6.1.5.5.7.48.1**<br>{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**<br>*(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**<br>*(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 |
| **certificatePolicies** | **policyIdentifier** | - | MS | **OID: 1.3.6.1.4.1.47718.2.1.2.2.1.10**<br>{ 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(10) } |
| | **policyQualifierID** | - | MS | Id-qt-1 (**CPS**) |
| | **qualifier** | - | MS | **https//repository.tsp.zetes.com** |
| | **policyQualifierID** | - | MS | Id-qt-2 (**User Notice**) |
| | **displayText** | - | MS | "**Enhanced normalized certificate for authentication as a natural person using a Secure Device.**" |
| | **policyIdentifier** | - | MS | **OID: 0.4.0.2042.1.2**<br>{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 Qualified Electronic Signature

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 algorithm for the key pairs is RSA2048. 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**

| | | | | |
|---|---|---|---|---|
| **certificate profile**<br>**ZETES TSP QCP-n-qscd certificate for natural persons - for the Subscriber OVB-OBFG**<br>**certificate policy OID: 1.3.6.1.4.1.47718.2.1.2.2.3.10**<br>**certificate profile OID: 1.3.6.1.4.1.47718.2.1.3.2.3.10**<br>version 1.0 | | | | |
| **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** |
| | **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**<br>This is a unique identifier (UUID) as assigned by OVB-OBFG. |
| | **title** | - | MD | **title of the Subject** as assigned by the SUB-RA/LRA<br>Dutch : "**advocaat**"<br>French : "**avocat**"<br>German : "**Rechtsanwalt**" |
| | **givenName** | - | MD | **official given name(s) of the Subject**<br>space (" ") separated full-form concatenation of given names, identical to how it is stated on the breeder document that was used to register the Subject |
| | **surName** | - | MD | **official surname(s) of the Subject**<br>space (" ") separated full-form concatenation of surnames, identical to how it is stated on the breeder document that was used to register the Subject |
| | **commonName** | - | MD | **the name of the Subject as assigned by the SUB-RA/LRA and an indication of the intended purpose for this certificate**<br>The format is a space separated concatenation of : |

| | | | | |
|---|---|---|---|---|
| | | | | • the label "**QES**" identifying the purpose of the certificate<br>• short-form surname of the Subject<br>• short-form given name of the Subject<br>• the title of the Subject in parentheses e.g. (advocaat) |
| | **countryName** | - | MD | **nationality of the Subject**<br>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<br>"**Orde van Vlaamse Balies (KBO 267.393.267)**"<br>or<br>"**Ordre des Barreaux Francophones et Germanophone de Belgique (BCE 850.260.032)**" |
| | **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**<br>{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) calssuers(2)} |
| | **accessLocation** | - | MS | **http://crt.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crt** |
| | **accessMethod** | - | MS | **OID: 1.3.6.1.5.5.7.48.1**<br>{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**<br>{ 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(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**<br>{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**<br>{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**<br>{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**<br>{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**<br>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**<br>*(URL of the web site with the Public Disclosure Statement in English)* |
| | **language** | - | MS | **en**<br>*(ISO 639-1 language code)* |
| | **url** | - | OS | **https://pds.tsp.zetes.com**<br>*(URL of the web site with the Public Disclosure Statement in Dutch)* |
| | **language** | - | OS | **nl**<br>*(ISO 639-1 language code)* |

| | | | | |
|---|---|---|---|---|
| | **url** | - | OS | **https://pds.tsp.zetes.com**<br>*(URL of the web site with the Public Disclosure Statement in French)* |
| | **language** | - | OS | **fr**<br>*(ISO 639-1 language code)* |
| | **url** | - | OS | **https://pds.tsp.zetes.com**<br>*(URL of the web site with the Public Disclosure Statement in German)* |
| | **language** | - | OS | **de**<br>*(ISO 639-1 language code)* |

## 7.2 CRL profile

Please read this document in conjunction with the corresponding Certification Practice Statement.

The Certification Practice Statement are published in the Zetes TSP repository on https://repository.tsp.zetes.com

## 7.3 OCSP profile

Please read this document in conjunction with the corresponding Certification Practice Statement.

The Certification Practice Statement are published in the Zetes TSP repository on https://repository.tsp.zetes.com

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Besides the supervision by the Belgian national supervisory body's (BeSign), ZETES TSP through its PMA organizes with regards to its CA activities a compliance audit to ensure that it meets requirements, standards, procedures and service levels according to its CPS [2].

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

Information about audit can be found in the CPS [2].

# 9 OTHER BUSINESS AND LEGAL MATTERS

The ZETES TSP Certificate Terms and Conditions constitute the main set of ZETES TSP standard terms and conditions for the provision and use of ZETES TSP Qualified CA's offering. For example, they provide general information about the conditions of use of ZETES TSP Certificates, the rights and obligations of ZETES TSP, the Subscribers and Relying Parties, including the duration and termination conditions, their liability, the claim process, or the applicable law and jurisdiction.

If and to the extent that ZETES TSP Qualified CA's offering is used in conjunction with other ZETES TSP services and products, the ZETES TSP Certificate Terms and Conditions must be read together with the terms and conditions governing the provision and use of these other ZETES TSP services and products.

The ZETES TSP Certificate Terms and Conditions apply each time the form or contract executed by the Subscriber or Subject (i) refers to the provision and use of ZETES TSP Certificates and (ii) expressly confirms that these ZETES TSP Certificate Terms and Conditions apply. A Relying Party not having executed any such form or contract shall be deemed to have tacitly accepted the ZETES TSP Certificate Terms and Conditions by relying or other acting upon a ZETES TSP Certificate.

The form or contract (if any) executed by Subscriber or Subject and the ZETES TSP Certificate Terms and Conditions, together with this Certificate Policy and the ZETES TSP Qualified CA Certification Practice Statement ("CPS") which are incorporated in the Certificate Terms and Conditions by reference, constitute the agreement between ZETES TSP and the Subscriber or Subject for the provision and use of ZETES TSP Certificates (the Agreement).

The sections below provide useful information about certain terms and conditions governing the provision or use of ZETES TSP Qualified CA's offering, as may be set out in more detail elsewhere in the Agreement.

## 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.

## 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 Certificate Terms and Conditions.

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.

The IPR with regards to Zetes acting as CSP, are ruled by the “Certificate Terms and Conditions”.

## 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 present CPS, 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 this 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 accepts 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 (S)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

### 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 CS 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 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

### 9.12.1 Procedure for amendment

ZETES TSP acting as CSP 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

Not applicable.

## 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 CPS (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----------**